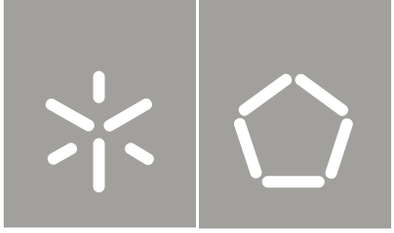
Universidade do Minho
Escola de Engenharia

Sidónio Micael Pereira de Seixas

Modelo para a Gestão de Eventos de Segurança da Informação

outubro de 2013

Sidónio Micael Pereira de Seixas Modelo para a Gestão de Eventos de Segurança da Informação
UMinho | 2013



Universidade do Minho
Escola de Engenharia

Sidónio Micael Pereira de Seixas

Modelo para a Gestão de Eventos de Segurança da Informação

Tese de Mestrado
Engenharia e Gestão de Sistemas de Informação

Trabalho efetuado sob a orientação do
Professor Doutor Henrique Manuel Dinis dos Santos

outubro de 2013

DECLARAÇÃO

É AUTORIZADA A REPRODUÇÃO INTEGRAL DESTA TESE APENAS PARA EFEITOS DE INVESTIGAÇÃO, MEDIANTE DECLARAÇÃO ESCRITA DO INTERESSADO, QUE A TAL SE COMPROMETE.

Guimarães, ___/___/_____

Assinatura: _____

Agradecimentos

Dedico esta dissertação, em particular, à Ana Isabel e à minha família por estarem sempre presentes e ajudarem dando a força e coragem necessária para continuar o trabalho desenvolvido. Agradeço também:

Ao professor Doutor Henrique Dinis dos Santos pela sua dedicação, ajuda e apoio sempre nos momentos mais complicados da realização da investigação e da própria dissertação;

Agradeço à Universidade do Minho por disponibilizar as ferramentas e espaços que foram necessários para a realização da investigação inerente a esta dissertação;

Ao Fábio, Cláudia e Manuel pela ajuda preciosa que forneceram para a realização da investigação inerente a esta dissertação;

Aos 34 gestores de segurança da informação que colaboram no *survey* de modo a que esse fosse possível ser realizado e, por consequência, fosse possível a realização da presente dissertação;

E por fim, a todos os que acreditavam em mim bem como a todos os que não acreditavam que eu era capaz de realizar esta dissertação.

Resumo

Com a rápida evolução tecnológica e o aparecimento de dispositivos com o objetivo de fornecer suporte aos sistemas de informação, a gestão de eventos de segurança da informação torna-se fundamental para garantir as propriedades básicas de segurança dos recursos críticos. Um Gestor de Segurança da Informação tem então que lidar com o aumento exponencial dos eventos (associados ao aumento do tamanho dos *logs* das aplicações), ao mesmo tempo que tem que compreender as diferentes causas subjacentes a cada um dos eventos detetados. Esta tarefa revela-se de uma complexidade enorme, bem para além da capacidade de resposta de um operador humano. Sendo assim, é de extrema importância o desenvolvimento de ferramentas que permitam, a um gestor, tratar os eventos de uma forma inteligente. Atualmente existem algumas soluções para esta área. No entanto, envolvem operações muito complexas de correlação de eventos e colaboração entre diversas entidades, preocupando-se com o foro tecnológico em detrimento do foro de perceção do gestor de segurança da informação, o que é manifestamente insuficiente. O objetivo desta dissertação passa pela descoberta de uma solução que permita, a um gestor, obter a perceção e controlo sobre os eventos de segurança da informação em tempo útil. Os objetivos são atingidos através a realização de um *survey* a 34 gestores de segurança da informação sendo que, com esse, foi permitido a elaboração de um conjunto de 6 requisitos para serem utilizados em ferramentas avançadas da área da Gestão de Eventos de Segurança da Informação (GESI). Com a apresentação dos 6 requisitos criados e aliando 9 dos 15 já definidos por diversos autores, criou-se um modelo GESI. Este pretende, inclusive, resolver alguns problemas identificados na área GESI como o aumento exponencial dos *logs* (com os eventos) sem terem a possibilidade de analisá-los devidamente, e a não deteção dos falsos positivos no sistema de segurança da informação criado.

Abstract

With the rapid technological evolution and the appearance of devices with the goal of providing support to information systems, security information event management (SIEM) becomes critical to ensure the critical resources security. An information security manager must deal with the event exponential increase (associated with the increase of logs applications size), and at the same time it has to understand the different causes that are associated with the detected events. This task is complex well beyond the response capability of a human operator. Therefore, it is extremely important to develop tools that allow a manager to deal with events with a smart way. Currently there are some solutions for this area. However, they involve complex event correlation events and various entities collaboration. This entities are concerned with the technological perception and not to the needs of information security manager. It's insufficient. The goal of this thesis involves the discovery of a solution that an information security manager use get the perception and control over the information security event in a short timeline. The objectives are achieved through the realization of a survey. 34 information security managers, have replied to the survey. With the information replies, was allowed to elaborate a set of six requirements for advanced tools. With this requirements and with nine of fifteen requirements that was proposed by others authors, was created an information security event management model. The model also aims to solve some problems identified in the information security event area like the logs the exponential increase (with events) without having the possibility to analyze them properly. Also aims to resolve the false positives none detection in the information security system.

Índice

Acrónimos

Tabela 1 – Acrónimos utilizados na dissertação

Acrónimo	Descrição
CALM	*Compromise and Attack Level Monitor*
CCSS	*Common Configuration Scoring System*
CIA	Confidencialidade, Integridade e Disponibilidade
COSO	*Committee Of Sponsoring Organisations of the Treadway Commission*
CVE	*Common Vulnerabilities and Exposures*
CVSS	*Common Vulnerability Scoring System*
DS	*Design Science*
DoS	*Denial-of-Service*
ENISA	*European Union Agency for Network and Information Security*
FIPS	*Federal Information Processing Standards*
FISMA	*Federal Information Security Management* Act
GESI	Gestão de Eventos de Segurança da Informação
GSI	Gestão de Segurança dos Sistemas de Informação
HIPAA	*Health Insurance Portability And Accountability Act*
IDS	*Intrusion Detection Systems*
IEEE	*Institute of Electrical and Electronics Engineers*

IPS	*Intrusion Prevention Systems*
ISMS	*Information Security Management System*
ISO/IEC	*International Organization for Standardization / International Electrotechnical Commission*
NES	Número de Eventos por Segundo
NIST	*National Institute of Standards and Technology*
ONU	Organização das Nações Unidas
OSSIM	*Open Source Security Information Management*
PCI	*Payment Card Industry Data Security Standard*
PDCA	*Plan-Do-Check-Act*
SEM	*Security Event Management*
SGSI	Sistema de Gestão da Segurança da Informação
SIEM	*Security Information Event Management*
SIM	*Security Information Management*
SOX	*Sarbanes-Oxley Act*
SR	*Survey Research*
TI	Tecnologias da Informação
VAAL	*Vulnerability Assessment Assurance Levels*
WAVS	*Web Application Vulnerability Scanners*

Lista de Figuras

Lista de Tabelas

1. Introdução

Nesta era tecnológica, as organizações utilizam a internet como um instrumento fundamental para a sua atividade. A informação que é gerada por estas ações é abundante e circula na internet gerando um número de eventos extremamente elevado. Contudo as organizações não podem ter o controlo total sobre o meio de processamento e armazenamento que utilizam aumentando assim drasticamente o risco associado à informação crítica.

A criação de normas constitui um importante passo para tentativa de controlar a segurança da informação crítica organizacional. Dessas normas salientam-se: a ISO/IEC 27004:2009 como sendo um dos guiões que permite implementar, nas organizações, um *Information Security Management System* (ISMS) através de componentes já retratados na ISO/IEC 27001:2009 (ISO/IEC, 2009a); a NIST SP-800-55, que se constitui como um guia de assistência para o desenvolvimento, seleção e implementação de métricas que são utilizadas pelos níveis do *software* para a segurança da informação (Chew et al., 2008); o *Payment Card Industry Data Security Standard* (PCI) que normaliza e assegura a segurança da informação dos pagamentos bancários (Hong Kong Government, 2008); ou a *Federal Information Processing Standards (*FIPS) que define controlos apropriados para diversas áreas (Hong Kong Government, 2008),

A criação de regulamentações específicas reflete, também, a necessidade que as organizações têm de ter as suas estruturas bem delineadas. As mais conhecidas são criadas nos Estados Unidos da América (EUA). A *Sarbanes-Oxley Act* (SOX), que permite a proteção dos investidores, o *Health Insurance Portability And Accountability Act* (HIPAA) que permite uma melhoria na portabilidade e continuidade da cobertura dos seguros de saúde prevenindo a perda da informação dos investidores e a *Federal Information Security Management Act* (FISMA) que impõe exigências que têm de ser compridas pelas agências governamentais norte americanas. Contudo os ataques têm continuado (Hong Kong Government, 2008).

Nos últimos anos tem vindo a aumentar o número de ciberataques. No ano de 2012, a nível nacional, por exemplo, são divulgados os dados de 25 árbitros da primeira

categoria de futebol. Informações como números de telemóvel, de identidade, de contribuinte, de identificação bancária; moradas da residência, do trabalho; endereço do correio eletrónico pessoal, profissão e até nomes de familiares foram divulgadas (Andrade e Oliveira, 2012). Outro ataque é direcionado ao Governo Português. A rede informática, em Agosto de 2012, foi alvo de 801.001 tentativas de ataques. O Governo não sabe quantas têm sucesso (Séneca, 2012). A nível internacional, por exemplo, a McAfee emite um comunicado onde explica um ciberataque que efetuou-se durante 5 anos seguidos a mais de 70 entidades. Uma das entidades é a Organização das Nações Unidas (ONU) que fica com a sua informação confidencial crítica exposta durante dois anos (os atacantes conseguiram aceder a diversos dados secretos da instituição). Outro dos ataques é documentado pelas empresas *Check Software Techologies* e a *Versafe*. Essas afirmam que detetaram um *botnet* (chamado *Eurograbber*) que efetua roubos na ordem dos 36 milhões de euros de contas de mais de 30 mil clientes bancários em quatro países europeus (Laxmidas, 2012; Pedro, 2012).

Estes ataques despoletam eventos de segurança. Esses ocorrem, em elevado número, nos sistemas de segurança existentes atualmente (como *firewall*, antivírus, sistemas operativos, *Intrusion Detection Systems* (IDS), *Intrusion Prevention Systems* (IPS), entre outros). Proporcionam um aumento exponencial do tamanho dos *log* desses mesmos sistemas. Esta situação torna a análise praticamente impossível. Alguns investigadores (como o Pearlman e Rheingans (2007) ou o Davey et al. (2012)) propõem soluções para a análise dos *logs* tendo por base a visualização da informação de segurança. Contudo as soluções que apresentam são demasiado técnicas (contem informação técnica e de difícil análise para um gestor que pode não ser dotado de elevadas capacidades técnicas) não sendo possível encontrar nenhuma solução com um foco claro na Gestão da Segurança da Informação (GSI). Existem soluções, denominadas de *Security Information Event Management* (SIEM), que permitem analisar ficheiros *logs* que possibilitam, através dos eventos de segurança da informação, a descoberta de ataques (Haymarket Media, 2013). As soluções contêm informação com características técnicas e que não vão de encontro ao que os gestores de segurança da informação necessitam na área dos eventos de segurança da informação. Verifica-se a necessidade da criação de uma solução que permita aos

gestores, claramente, controlar os eventos de segurança da informação em tempo útil. Se os eventos são devidamente tratados/geridos, acredita-se que podem fornecer informação útil a um gestor de modo a que esse possa evitar ou mitigar a ameaça associada.

Como resposta aos problemas retratados, esta dissertação apresenta um Modelo de GESI. Esse modelo baseia-se em seis requisitos, que são retirados de um *survey* realizado no âmbito desta dissertação. Com base no *survey*, garante-se que o modelo contempla o que os gestores de segurança da informação realmente necessitam no âmbito da análise dos eventos de segurança da informação.

1.1 O Problema na Gestão de Eventos de Segurança da Informação

Os eventos de segurança que são despoletados nas organizações, aumentam a cada segundo que passa. Reportam diversos ataques que são efetuados aos sistemas de informação sendo difícil para um gestor de segurança da informação definir medidas para tentar travar ou mitigar as suas ameaças. Os eventos podem ser de foro interno (máquinas internas na organização), sendo que esses podem ser de natureza criminosa ou involuntária, ou de foro externo (máquinas externa à organização).

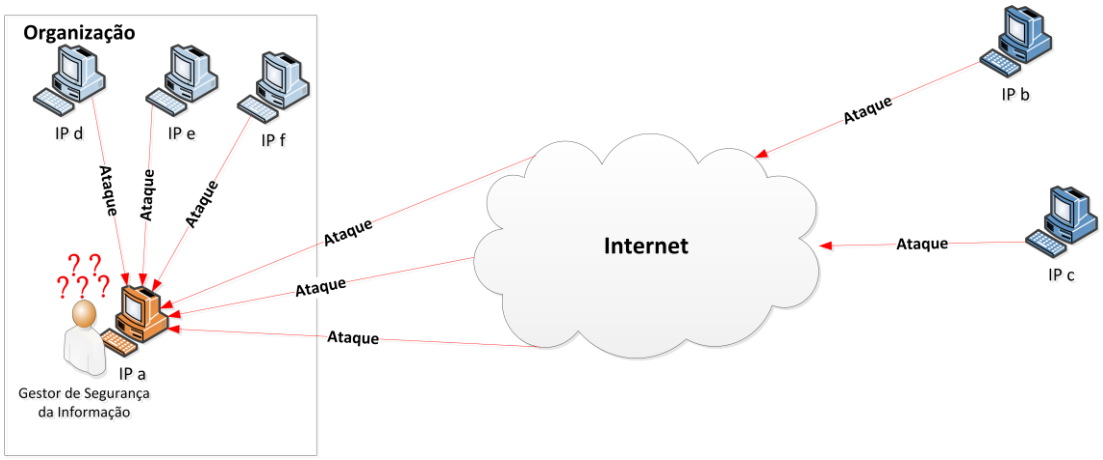


Figura 1 – Problema da análise manual de eventos de segurança da informação

Com base na Figura 1, verifica-se a ocorrência de três ataques internos, provenientes dos Endereços IP “IP d”, “IP e” e “IP f”, e dois ataques externos, provenientes dos Endereços IP “IP c” e “IP d”. O “IP a”, a máquina do gestor, contém a informação dos ataques em diversos ficheiros existentes nos sistemas de segurança que possui (exemplos: *logs* de *firewall*, antivírus, IDS entre outros). Contudo, essa informação está dispersa por diversos sistemas e, normalmente, é de difícil interpretação (devido à sua natureza técnica). Através da Figura 1, tipicamente, verifica-se o que se passa dentro de uma organização ao nível da segurança da informação. Contudo numa organização real não são seis máquinas a interagir mas centenas de máquinas em constante comunicação. Pode-se afirmar que o número de eventos por segundo (NES) pode ser extremamente elevado.

A *European Union Agency for Network and Information Security* (ENISA), entidade europeia para a segurança da informação, anualmente produz um relatório com uma análise sobre os incidentes que ocorrem no sector das comunicações. No relatório de 2012, a ENISA menciona os cibertaques como sendo uma das causas dos incidentes e que têm aumentado. De 2011 para 2012 os incidentes causados por ciberataques subiram 4% (de 2% para 6%). Cerca de 1.8 milhões de comunicações foram afetadas (Dekker et al., 2012)

O aumento dos incidentes, que pressupõe que haja um aumento de eventos de segurança da informação, agrava assim o problema retratado nesta subsecção. Em acréscimo, não existem relatos de nenhum estudo que transmita o que um gestor de segurança da informação realmente pretende ver no âmbito da GESI de modo a minimizar o impacto na sua organização.

1.2 Objetivos

A presente dissertação, como qualquer estudo, tem objetivos associados. O objetivo desta dissertação passa pela descoberta de uma solução que permita apoiar um gestor de segurança da informação no âmbito da GESI. Essa solução permitirá aos gestores: 1 – Analisar os eventos de segurança da informação que ocorrem nas organizações; 2 – Perceber concretamente o que se passa com a segurança das organizações; 3 –

Mitigar os impactos que advém dos eventos que ocorrem nos sistemas das organizações. Para que seja possível atingir este objetivo, define-se dois sub-objetivos:

1. Levantamento de requisitos de um gestor de segurança da informação. O levantamento dos requisitos de um gestor é efetuado através do *survey* e permite que sejam definidas as dimensões que são utilizadas na solução que é proposta;
2. Criação e definição de um modelo para a GESI. A criação e definição de um modelo de GESI, permite a um gestor lidar com os eventos de segurança que ocorrem sobre a sua informação crítica de modo a tomar a decisão certa para tentar, no mínimo, minimizar os estragos efetuados sobre a informação.

Espera-se, com esta dissertação, a identificação das necessidades que os gestores de segurança da informação têm no âmbito dos eventos de segurança da informação. Como contributo espera-se a criação e definição de um modelo para a GESI que permita a investigadores e organizações a criação e implementação de novas soluções nesta área.

1.3 Abordagem Metodológica

Para atingir-se os objetivos propostos utiliza-se uma metodologia de investigação, a *Design Science* (DS), e um método de investigação, o *Survey Research* (SR). A DS foi selecionada porque, para responder ao objetivo principal identificado, irá ser criado um artefacto, o modelo para GESI. O SR, integrado na metodologia de investigação *Quantitative Positivist Research* (Vaishnavi e Kuechler, 2004), foi selecionado pois é necessário efetuar um levantamento das necessidades dos gestores de segurança da informação no âmbito da análise dos eventos de segurança da informação.

A abordagem DS aplica-se ao longo de toda a investigação enquanto o SR aplica-se num momento particular da investigação, concretamente no segundo passo da metodologia DS (Figura 2).

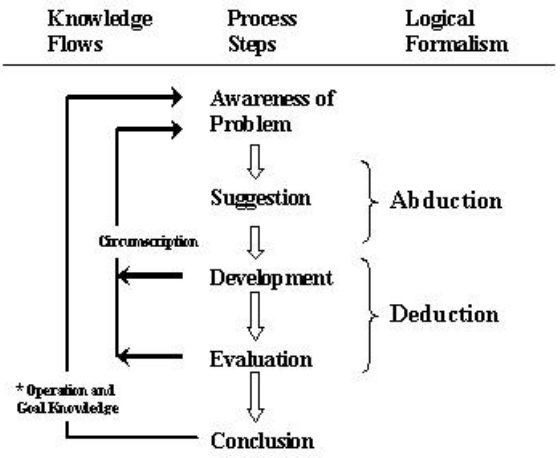


Figura 2 – Metodologia DS (Fonte: Vaishnavi e Kuechler (2004))

Como se pode visualizar pela Figura 2, a abordagem DS é constituída por 5 passos principais: reconhecimento do problema, sugestão, desenvolvimento, avaliação e conclusão.

Alguns investigadores, para a utilização da metodologia DS, mencionam algumas orientações. Hevner et al. (2004) estabelecem sete orientações para a abordagem DS: artefacto, relevância do problema, rigor na investigação, *design* como um processo de investigação, avaliação do design, contribuições da investigação e comunicação da investigação. No âmbito desta dissertação opta-se pela utilização destas orientações. Esta opção permite que seja aplicada a metodologia DS de modo a que se atinja o artefacto identificado, ou seja, o modelo de GESI. As orientações estão descritas Tabela 2.

Tabela 2 – Descrição das sete orientações (Baseado em: Hevner et al. (2004))

Orientação	Descrição
Artefacto	Modelo para a GESI com base nas necessidades levantadas pelo *survey*

	efetuado aos gestores de segurança da informação. Este levantamento é efetuado através da aplicação do método científico SR.
Relevância do problema	Com base nos problemas mencionados anteriormente aumenta o grau de dificuldade para a GESI. Os SIEM são as ferramentas utilizadas para a GESI. Contudo são ferramentas com uma análise dos eventos de segurança da informação técnica e de difícil perceção por um gestor de segurança da informação (que não seja proveniente de área técnica). Torna-se necessária a criação de um Modelo de GESI baseado nas necessidades de um gestor no âmbito dos eventos de segurança da informação. Este modelo permite que exista uma perceção sobre a segurança da informação da organização.
Avaliação do *Design*	A avaliação é efetuada através da aplicação do modelo sobre tráfego num regime controlado. Posteriormente efetua-se uma análise dos resultados.
Contribuições da Investigação	A utilização do modelo de GESI, por organizações, permitirá aos gestores de segurança da informação uma análise dos eventos de segurança da informação mais eficaz. Ao nível da utilização, por parte dos investigadores, o modelo de GESI pode apresentar-se como ponto de

	partida para a criação e desenvolvimento de novas investigações (nomeadamente ao nível da definição de dimensões de análise e visualização) na área da GESI.
Rigor da Investigação	A investigação é efetuada de acordo com metodologias de investigação reconhecidas.
Processo de Pesquisa	Inicia-se com a pesquisa sobre vários conceitos relevantes na área da GSI e concretamente na área dos eventos de segurança da informação. Seguidamente efetua-se a pesquisa sobre trabalhos existentes na área dos eventos de segurança da informação de modo a produzir-se o *survey*. Após a existência de resultados do *survey*, efetua-se uma análise detalhada para extrair as informações relevantes para a criação do modelo (artefacto).
Comunicação da Investigação	O resultado do estudo e desta dissertação irá ser publicado na biblioteca da Universidade do Minho para consulta gratuita por toda a comunidade.

1.4 Mapa do contexto do estudo da Dissertação

Através de um mapa do contexto do estudo da dissertação pode-se verificar o trabalho de investigação efetuado (Figura 3).

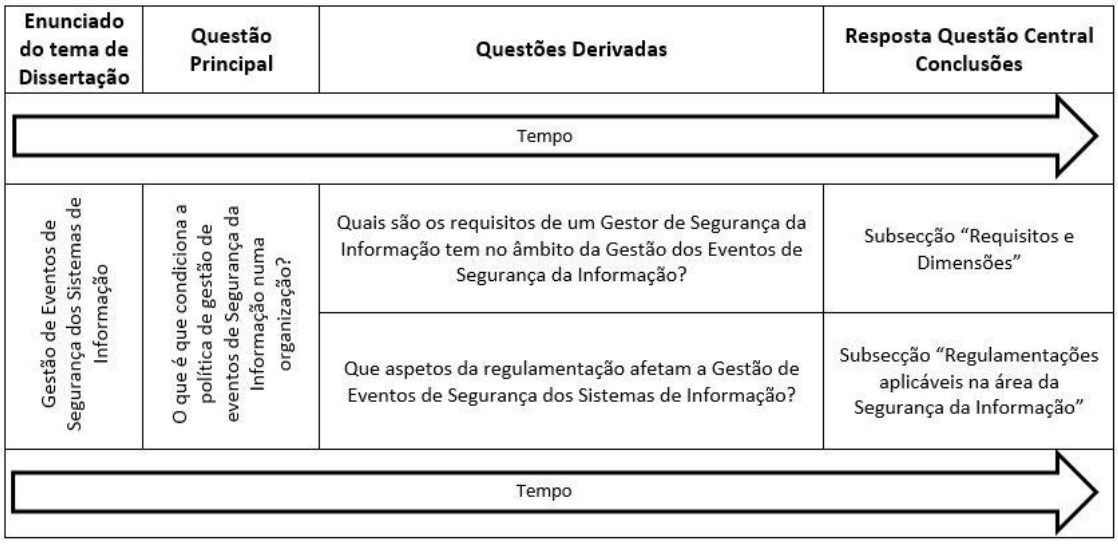


Figura 3 – Mapa do contexto do estudo da Dissertação

Verifica-se a constituição de uma questão principal seguida de duas questões derivadas dessa. Através da coluna "Resposta Questão Central Conclusões" consegue-se identificar qual é a secção ou subsecção que contem a resposta a determinada questão.

1.5 Estratégia de Pesquisa no Âmbito da Dissertação

Com a questão de investigação definida, torna-se necessário a definição de uma estratégia de pesquisa para atingir uma resposta à mesma. Essa pesquisa permite a obtenção de uma perceção do problema e permite, inclusive, uma visão sobre o que os investigadores têm feito na área da GESI.

A estratégia definida passa pela seleção de palavras-chave que são utilizadas para a pesquisa dos conceitos teóricos, normas e regulamentações e para a pesquisa de trabalhos efetuados no âmbito da definição de requisitos para os SIEM e para a visualização de informação de segurança (Tabela 3).

Tabela 3 – Palavras-chave para a pesquisa no âmbito da dissertação

Palavras-Chave
Sistema de Gestão da Segurança da Informação / *Information System Security Management*
Segurança da Informação / *Information Security*
Evento / *Event*
Security Information Event Management (SIEM)
Políticas de Segurança da Informação / *Information Security Politics*
Número de Eventos por Segundo / *Event per Second* / EPS
Criticidade dos eventos de segurança da informação / *Information Security Event Criticity*
Normas para eventos de segurança da information / *Event information security standards*
Regulamentação para segurança da informação / *regulation for information security*
Vulnerabilidades e eventos de segurança da informação / *Vulnerabilities and information security event*
Visualização de eventos / *Events*

visualization
Eventos de segurança / *Security events*
Análise dos dados dos eventos de segurança da informação / *Information security event Data Analysis*
Sistemas de visualização de informação de segurança / Information Security v*isualization systems*

As palavras-chave selecionadas tiveram por base a área do estudo da presente dissertação, eventos de segurança da informação, e a questão de investigação anteriormente definida. Após a sua seleção efetua-se a pesquisa, analisa-se os documentos e aplicam-se cinco critérios rigorosos (Tabela 4). Note-se que foram extraídos cerca de cinquenta documentos, através das palavras-chave, aos quais foram aplicados os critérios restando seis artigos.

Tabela 4 – Os cinco critérios de pesquisa

Nome	Descrição	Critério (s)
Ano	Os artigos selecionados estão datados num período de cinco anos. A seleção foi efetuada devido a existir elevadas alterações tecnológicas de um ano para o seguinte.	De 2007 a 2013.
Titulo relevante	Tem de referenciar conceitos relativos a SIEM, gestão de eventos de segurança da informação, eventos de	Existência de algumas das seguintes palavras: Evento, *event*, gestão da segurança da informação, gestão de eventos

	segurança da informação, requisitos para sistemas de segurança, Data Mining.	de segurança dos sistemas de informação, *security event management*, SIEM, ISMS, *Visualization, security, security assessment, security, event management.*
Abstract relevantes	Tem de referenciar as palavras-chave, ou sinónimos, detalhadas na Tabela 3.	Existência de algumas das seguintes palavras: *Security Information Event Management (SIEM); Events Visualization; Security Events; Event Data Analysis; Data Mining; Visualization systems.*
Keywords relevantes	Tem de referenciar as palavras-chave, ou sinónimos, detalhadas na Tabela 3.	Existência de algumas das seguintes palavras: *Security Information Event Management (SIEM); Events Visualization; Security Events; Event Data Analysis; Data Mining; Visualization systems.*
Conferências ou revistas científicas	Terão que estar referenciados, os artigos, em revistas que publiquem na área em estudo.	IEEE, *Springer, ScienceDirect, Association for Computing Machinery, Academic Conference Internacional*, ACM.

Com a aplicação dos cinco critérios (Tabela 4) foram selecionados sete documentos científicos que estão compreendidos entre os anos de 2007 e 2012 (um documento de 2007, um documento de 2008, um documento de 2011 e quatro de 2012). Note-se que poderão ter escapado alguns documentos científicos que sejam referentes a esta

área, contudo com os critérios estabelecidos, não foram selecionados e, por consequência, analisados.

1.6 Estrutura do documento de Dissertação

A presente dissertação está estruturada em 5 capítulos. O capítulo Introdução menciona o problema detetado na gestão de eventos de segurança da informação e a sua relevância, os objetivos a atingir e a questão central da investigação a efetuar, a abordagem e métodos científicos a utilizar, os cenários que podem ocorrer e que comportam algum risco para a realização da dissertação, o diagrama de contexto, bem como todo o planeamento e estrutura da investigação que culmina com a realização desta dissertação. O capítulo Gestão de Eventos de Segurança da Informação refere todos os conceitos, normas e regulamentações que são necessários para a realização desta dissertação, bem como trabalhos científicos importantes realizados sobre o tema da visualização de dados e dos requisitos para os SIEM. O capítulo Modelo para a Gestão de Eventos de Segurança da Informação apresenta o *survey* e os requisitos e dimensões baseados no mesmo. Apresenta ainda o modelo criado, com base nos requisitos e dimensões definidas e mencionadas anteriormente. O capítulo Discussão e Conclusão apresenta uma discussão sobre a temática abordada e as conclusões a que o estudo permite chegar. O último capitulo, Investigação Futura, reflete algumas diretrizes que podem ser seguidas com base no trabalho apresentado.

2. Gestão de Eventos de Segurança da Informação

O foco da presente dissertação é a resolução do problema identificado na área da GESI. Os conceitos fundamentais, as normas, a regulamentações e os trabalhos efetuados no âmbito dos eventos de segurança da informação estão descritos neste capítulo.

2.1 Conceitos Fundamentais, Normas e Regulamentações

De modo a ser possível a obtenção de uma análise profunda sobre o problema identificado é estritamente necessário o conhecimento de alguns conceitos, normas e regulamentações (HIPAA e SOX). Os que são apresentados nesta dissertação são oriundos dos Estados Unidos da América (EUA).

2.1.1 Conceito de Segurança da Informação

A Segurança da Informação é definida na norma ISO/IEC 27000:2009 como sendo a preservação da confidencialidade, integridade e disponibilidade (CIA) da informação. Além disso, outras propriedades como a autenticidade, o não-repúdio, a responsabilidade e a confiabilidade podem, também, estar envolvidos (ISO/IEC, 2009b).

2.1.2 Conceito de Evento de Segurança da Informação

Como é evidente, este conceito é de extrema relevância para a área abordada. Para se conseguir perceber procura-se entender o que é um evento no contexto que se pretende abordar.

2.1.2.1 Evento

O Howard e Longstaff (1998) afirmam que o *Institute of Electrical and Electronics Engineers* (IEEE) propõe uma definição para evento: um evento é uma mudança discreta do estado ou condição de um sistema ou dispositivo. Esse evento resulta de ações que ocorrem contra sistemas de informação. Um exemplo simples de um evento corresponde ao momento de autenticação de um utilizador numa máquina. Primeiro, ocorre uma mudança de estado no Sistema de Informação. No caso em particular, o alvo no Sistema de Informação seria a conta do utilizador (Howard e Longstaff, 1998). Os dois autores referem uma matriz de ações e alvos que podem representar possíveis eventos computacionais ou de rede (Figura 4).

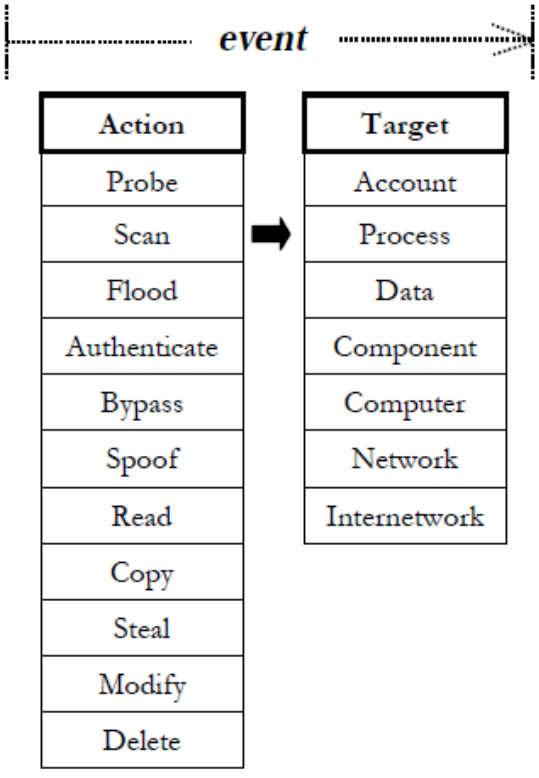


Figura 4 – Eventos de Rede e Computacionais[1] (Fonte: Howard e Longstaff (1998))

[1] Tradução livre de *network events*

Com base nesta matriz e na definição do IEEE, Howard e Longstaff (1998) definem evento como sendo uma ação dirigida a um alvo que tem como objetivo a alteração de um estado (*status*) do alvo. Para existir um evento, é necessário que exista uma ação e, mais ainda, que essa ação seja dirigida a um alvo. O evento, inclusive, constitui uma representação lógica entre uma ação e um alvo específico. Contudo, a definição apresentada e defendida pelos dois autores não permite efetuar a distinção entre as ações autorizadas e não autorizadas (a maioria dos eventos são de rotina e são autorizados). Por isso, assumem todas as ações como eventos. É necessário referir que, no caso da Figura 4, nem todas as combinações entre a ação e o alvo são possíveis de acontecer no âmbito de um evento.

Com base nas definições apresentadas acima e restringindo ao contexto da segurança da informação, pode-se definir um evento de segurança da informação como sendo uma ação dirigida a um determinado alvo, dentro da organização, que tem como objetivo ultrapassar a proteção desse mesmo alvo alterando-lhe o seu estado. Esta definição vai de encontro à definição exposta na norma ISO/IEC 27000:2009: um evento de segurança da informação é uma ocorrência no sistema, serviço ou rede, não identificada no estado de um sistema, serviço ou rede, que indica uma possível quebra da política de segurança da informação, uma falha de segurança nos controlos, ou ainda, uma situação desconhecida previamente e que poderá ser relevante a nível da segurança (ISO/IEC, 2009b).

2.1.3 Conceito de Número de Eventos por Segundo - NES

O NES reflete-se como um método para rever e avaliar as estatísticas de utilização de dispositivos de *hardware*, de *software*, de rede ou de segurança. Calcula-se como sendo o número de eventos, ou processos, que ocorrem num determinado período de tempo num determinado sistema (Cloud Access, 2011; Techopedia, 2013). O NES é uma componente da gestão de *log* de eventos, ou de *software*, que permite a monitorização de todos os eventos internos ou externos que são gerados pelo sistema. A sua utilização depende do ambiente no qual ele está a ser calculado (Techopedia, 2013). Para efetuar-se uma análise do NES existem duas métricas: a métricas dos eventos normais por segundo e a métrica do pico de eventos por

segundo. Através da primeira consegue-se verificar os eventos por segundo que podem ser considerados normais (ou seja, a ocorrência de eventos por segundo, em média, é aproximada). De acordo com a segunda, os eventos têm um pico (captura de número de eventos elevada) o que poderá indicar atividade anormal ou eventos suspeitos que podem gerar ataques ao sistema de informação (Cloud Access, 2011)

Segundo a Cloud Access (2011), para os SIEM, o NES, atualmente, é utilizado para calcular a necessidade de utilização dos SIEM nas organizações (tipicamente, é por esta via que os SIEM são debitados às organizações). Se não existe uma estimativa precisa do NES pode-se estar a sobre dimensionar ou subdimensionar os eventos que ocorrem no sistema de informação.

2.1.4 Conceito de Sistema de Gestão da Segurança da Informação - SGSI

O conceito de SGSI aqui apresentado tem relevância na área da segurança da informação. Apesar de esta dissertação estar vocacionada especificamente na área da GESI, o conceito tem relevância para o estudo. Um SGSI ou ISMS.

Para Eloff (2003) um SGSI é um sistema de gestão que tem como objetivo estabelecer e manter um ambiente seguro para a informação crítica de uma organização. Segundo o mesmo autor, esse sistema deve abordar a implementação e a manutenção de processos e procedimentos de gestão segurança das Tecnologias da Informação (TI). Como exemplos enuncia os seguintes: identificação das necessidades de segurança da informação numa organização e implementação de uma estratégia para atender a essas mesmas necessidades, a medição de resultados e o aperfeiçoamento das estratégias de proteção ao longo do tempo.

Ericsson (2004) define, com maior detalhe um SGSI. Um SGSI é constituinte integral de um sistema global de gestão de uma organização, tendo por base uma abordagem de risco para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação.

Martins e Santos (2005) definem um SGSI como sendo um sistema que, para as organizações, é análogo a um sistema de qualidade e, como tal, é passível de

certificação. Essa deve ser obtida a partir de evidências (documentos e práticas estabelecidas) sobre o conjunto de controlos que estão implementados e que devem ser executados e registados continuadamente ao longo do tempo.

A norma BS1799, substituída entretanto pela ISO/IEC 27001:2005, define um SGSI como um sistema baseado no ciclo contínuo de atividades, o *Plan-Do-Check-Act* (PDCA). Um SGSI funciona como um modelo cíclico que visa assegurar que as melhores práticas de uma organização são documentadas, reforçando e melhorando a organização ao longo do tempo (citado por Eloff e Eloff, em 2005). Esse modelo é constituído por quatro fases principais (Figura 5).

No decorrer de 2012, Gilaninia et al. define SGSI como sendo uma parte de um sistema de gestão organizacional abrangente e que esse é baseado em estimativas e análises de risco. Esse sistema irá ser utilizado para projetar, implementar, administrar, monitorar, rever, manter e melhorar a segurança da informação. A sua aplicação tem forçosamente impacto nos objetivos e exigências da organização, nos requisitos de segurança, nos procedimentos adotados e no tamanho e estrutura da organização.

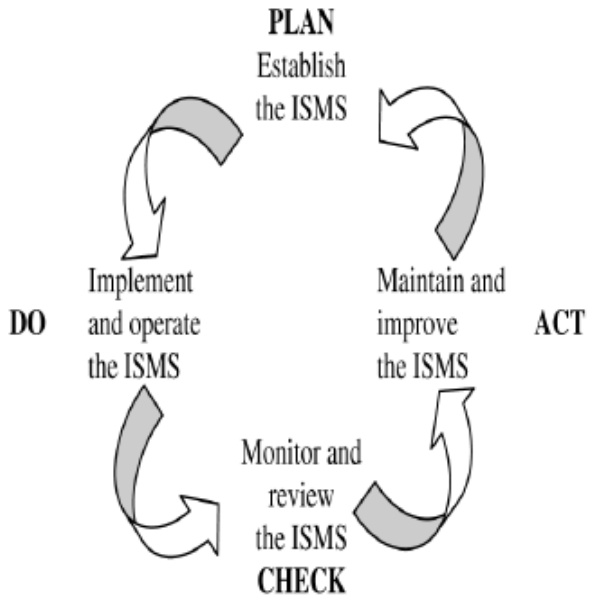


Figura 5 – Modelo PDCA aplicado aos processos de um SGSI (Fonte: Eloff e Eloff (2005))

O objetivo de um SGSI constitui-se como sendo a proteção da informação crítica de uma organização através da análise da confidencialidade, precisão e disponibilidade (Figura 6). O artefacto que resulta da implementação de um SGSI é a padronização e documentação dos procedimentos, ferramentas e técnicas utilizadas pela organização bem como a definição de um processo educacional e de consciencialização dentro da organização (Martins e Santos, 2005).

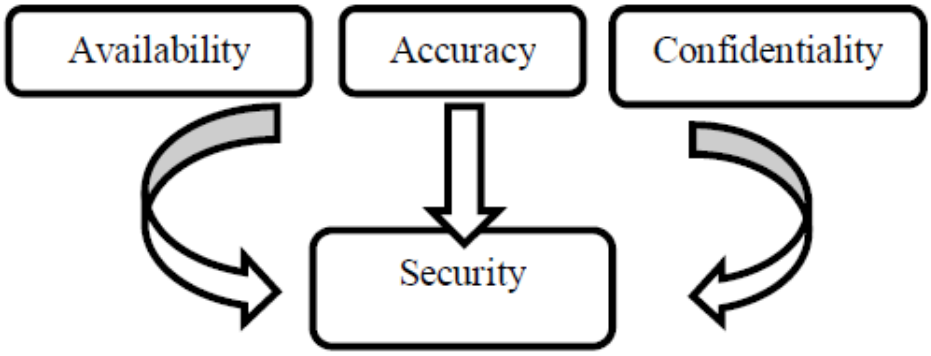


Figura 6 – Objetivo de um SGSI (Fonte: Gilaninia *et al.* (2012))

2.1.5 Conceito de Criticidade dos Eventos de Segurança da Informação

A criticidade permite a valorização dos eventos de segurança da informação de forma a priorizar os eventos, de acordo com a sua importância, em função do sistema a monitorizar (Rocha, 2013).

2.1.6 Conceito de Política de Segurança da informação

A política de segurança, nas organizações, constituem-se como um controlo de segurança da informação (J.Kenneth et al., 2009). Essas políticas são um primeiro passo para preparar as organizações contra os ataques, internos ou externos, que possam vir a decorrer na organização (Whitman et al., em 2001, citado por

J.Kenneth et al. (2009)). Para além de permitirem uma abordagem ao CIA, as políticas de segurança da informação são uma vertente clara de gestão e contribuem para uma formação dos colaboradores de modo a que esses sejam sensibilizados para a segurança da informação (Wood, em 1995, citado por J.Kenneth et al. (2009)). As organizações devem estabelecer e manter um processo de políticas de segurança da informação, assente em bases sólidas, de modo a que a proteção da informação seja eficaz (J.Kenneth et al., 2009).

2.1.7 Conceito de Security Information and Event Management - SIEM

Os SIEM são utilizados pelas organizações para gerir eventos de segurança da informação, como o próprio nome indica. Segundo Tangil et al. (2013) um SIEM é um sistema que se traduz numa solução holística para uma organização que organiza e correlaciona informação de segurança. Pode também ter uma definição mais técnica. Assim é definido como um *software* que analisa ficheiros *logs* para descobrir ataques invisíveis aos seus dados (Tangil et al., 2013). Tem como objetivo a optimização do tempo dispensado pelos administradores de segurança e assim melhorar a resposta a incidentes. Nos últimos anos têm aparecido diversas soluções SIEM, como o ArcSight, o *RSA*, o *Novell - IBM*, o *SenSage* ou o *Alien Vault* (Figura 7). Este tipo de soluções, segundo Nicolett e Kavanagh (2011), fornecem:

- Uma componente de *Security Information Management* (SIM): que permite a gestão de *logs* e relatórios de conformidade com normas e regulamentações;
- Uma componente *Security Event Management* (SEM): permite a monitorização em tempo real dos eventos bem como a gestão de incidentes relacionados com os eventos captados na rede, nos sistemas de segurança, nos sistemas operativos e nas aplicações.

A sua utilização, normalmente recai sobre a conformidade - gestão de *logs* e relatórios de conformidade, e a gestão de incidentes - monitorização em tempo real da atividade dos utilizadores, acesso a dados, atividade das aplicações e gestão de incidentes (Nicolett e Kavanagh, 2013).

Figura 7 – SIEM comercializados a nível mundial (Fonte: Nicolett e Kavanagh (2013)

Um SIEM pode ser utilizado para diversas finalidades dentro de uma organização. Haymarket Media (2013) menciona as seguintes: detetar uma violação da política de segurança e obter relatórios; efetuar correlação de diversos eventos; obter uma consola integrada e que permita visualizar os eventos em tempo real fazendo com que as respostas sejam mais rápidas; descobrir *malwares*; modelação de segurança; e investigação forense.

Viera et al. (2012), na seu projeto de graduação, afirmam que um SIEM, no caso o *Open Source Security Information Management* (OSSIM), permite calcular a

evolução dos riscos, efetuar correlação de eventos, obter indicadores de risco, analisar vulnerabilidades, efetuar *data mining* sobre os dados e monitorizar em tempo real os eventos. Este tipo de sistemas, normalmente, é destinado para administração de *logs*, correlação de eventos e respostas ativas e rápidas.

2.2 Normas para a Segurança da Informação

As normas providenciam um guião que permitam a construção de métricas e indicadores de modo a existir eficiência na organização (ISO/IEC, 2009a). A ISO/IEC e a *National Institute of Standards and Technology* (NIST) são entidades que, a nível mundial, operam na criação, manutenção e dissiminação de normas.

No âmbito desta dissertação, são referidas as normas ISO/IEC 27004:2009 e a NIST SP 800-55. Existem outras entidades que se debruçam sobre esta temática. Contudo essas são específicas para determinadas áreas de mercado. Exemplos dessas normas são: o PCI.

2.2.1 ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement

Esta norma é um dos guiões que permitem que seja implementado, nas organizações, um ISMS. Esta implementação assume componentes existentes na ISO/IEC 27001:2009 tais como politicas, gestão do risco da segurança da informação, objetivos de controlos, controlos, processos e procedimentos, e suporta a revisão dos processos (ISO/IEC, 2009a). A norma permite às organizações: avaliarem a eficiência dos controlos que têm sobre a sua segurança da informação; avaliarem a eficiência da implementação de SGSI (pressupõe-se que exista na organização); verificarem a métrica que indica se os requisitos de segurança definidos estão a ser cumpridos; ajuda na melhoria do desempenho da segurança da informação no que se refere a riscos de negócios, a nível global, praticados pela organização; e fornece dados para a gestão de modo a facilitar a tomada de decisão justificando assim as melhorias necessárias a implementar sobre o ISMS.

2.2.2 NIST Special Publication 800-55 Revision 1 - Performance Measurement Guide for Information Security

A norma foi criada com o objetivo de ser um guia de assistência para o desenvolvimento, seleção e implementação de métricas de modo a essas serem utilizadas pela segurança da informação (Chew et al., 2008). Essas métricas podem ser utilizadas para a tomada de decisão organizacional. Nesta situação, elas devem medir a recolha, análise e *report* dos dados organizacionais. Irá proporcionar uma forma de implementação da segurança da informação e dos controlos de segurança para as agências federais atingirem com sucesso a sua missão.

2.2.3 Payment Card Industry Data Security Standard

A PCI foi desenvolvida por organizações ligadas ao sector bancário com o objetivo de assegurar a segurança da informação de pagamentos efetuados por cartões de crédito. Esta norma define requisitos que se inserem dentro de diferentes áreas: contruir e manter uma rede segura; proteger dados dos cartões; efetuar manutenção de um programa de gestão de vulnerabilidades; implementar medidas severas para controlar os acessos à informação; monitorizar e testar redes regularmente; e implementar e manter as políticas de segurança da informação (Hong Kong Government, 2008).

2.2.4 Federal Information Processing Standards

As normas criadas pela FIPS são normas de segurança que tem em atenção a regulamentação FISMA (Hong Kong Government, 2008). Segundo o Governo de Hong Kong, em 2008, este conjunto de normas é transversal a 17 áreas. As áreas que são abrangidas vão desde o controlo de acessos, passando pelo *business plan continuity* até à integridade da informação.

As agências federais são obrigadas a obter os requisitos mínimos de segurança definidos para as áreas mencionadas através da seleção de controlos de segurança apropriados (Hong Kong Government, 2008).

2.3 Regulamentações aplicáveis na área da Segurança da Informação

Atualmente existem diversas regulamentações para todas as áreas. No caso da segurança da informação, no âmbito esta dissertação opta-se por referenciar duas regulamentações: a HIPAA e a SOX. A escolha destas regulamentações é efetuada com base na importância que o mercado da Saúde e da Imobiliária têm no mercado dos Estados Unidos da América.

2.3.1 Health Insurance Portability And Accountability Act

HIPAA é uma regulamentação criado pelos EUA no ano de 1996. Esta regulamentação tem como objetivo conceder uma melhoria na portabilidade e continuidade da cobertura dos seguros de saúde nos mercados designados por mercado de grupo e mercados individuais. Permite um combate ao desperdício, fraude e abuso das vantagens do seguro de saúde (Hong Kong Government, 2008). A regulamentação define os padrões de segurança da informação para a área da saúde levando em conta uma serie de fatores. Nesses são incluídas as capacidades técnicas dos sistemas de registos de utilizadores, o custo das medidas de segurança, a necessidade de formação de colaboradores, o valor das auditorias a efetuar e as necessidades e capacidades dos fornecedores. As pessoas que transmitem ou mantêm informação de saúde são obrigadas a mantê-las guardadas administrativamente, técnica e fisicamente de modo a garantir a integridade e confidencialidade das mesmas. A HIPAA obriga as organizações a monitorizarem os eventos associados à utilização da segurança na área da saúde. Esta regulamentação pode ser consultada no *site* governamental dos EUA, nos *US Department of Health and Human Services* (Hong Kong Government, 2008).

2.3.2 Sarbanes-Oxley Act

A SOX é uma regulamentação criada pelos EUA no ano de 2002. O objetivo é a proteção dos investidores através da melhoria da precisão e confiabilidade das divulgações cooperativas efetuadas de acordo com as leis de valores imobiliários nos EUA. O SOX aparece após um número considerável de escândalos empresariais (Hong Kong Government, 2008). Nesta regulamentação, diretamente, não estão especificadas requisitos de segurança da informação. Contudo, denota-se que, para cumprir esta regulamentação, não existe nenhuma forma de um sistema financeiro continuar a fornecer informações financeiras fiáveis sem existir medidas de segurança da informação apropriadas e diversos controlos em locais específicos do fluxo da informação (Hong Kong Government, 2008).

A *Committee Of Sponsoring Organisations of the Treadway Commission* (COSO) é utilizada, normalmente, em conjunto com o SOX de modo a satisfazer a conformidade exigida às organizações (Hong Kong Government, 2008). Constitui-se como sendo uma *framework* que inicia um processo de controlos internos nas organizações. Esta *framework* tem como objetivo ajudar as organizações, no processo de controlo, avaliando a eficácia dos controlos internos (Hong Kong Government, 2008). Segundo o Governo de Hong Kong (2008), a COSO contém cinco componentes:

1. Ambiente de Controlo. Inclui fatores como a integridade das pessoas dentro da organização ou a autoridade e responsabilidade na gestão de determinadas áreas, infraestruturas, entre outros;
2. Avaliação do Risco. Permite a identificação e avaliação dos riscos que podem prejudicar o negócio da organização;
3. Controlo das atividades Organizacionais. Estão incluídas as políticas e os procedimentos adotados pela organização;
4. Informação e Comunicação. Permite identificar a informação organizacional crítica para o negócio e os canais de comunicação para a criação de medidas de controlo para a gestão dos colaboradores;
5. Monitorização. Inclui o processo utilizado para avaliar a qualidade de todos os controlos no sistema da organização ao longo do tempo.

2.4 Avaliação e Classificação de Eventos de Segurança da Informação

Com o NES a aumentar todos os dias nas organizações, torna-se fundamental que hajam ferramentas, métodos de classificação ou *framework* para que seja possível a otimização dos chamados falsos positivos. Estas permitem a um colaborador de uma organização, ligado à área, avaliar e classificar eventos de segurança da informação que ocorrem no sistema de informação do seu empregador. Alguns desses casos são referenciados na presente dissertação.

2.4.1 Common Vulnerabilities and Exposures

A CVE é um dicionário público onde constam os nomes das vulnerabilidades que afetam a segurança da informação (Mitre, 1999). Foi constituída em 1999 quando a maioria das ferramentas de segurança tinham a sua própria base de dados de vulnerabilidades. Naquela época, era impossível verificar se diferentes bases de dados continham as mesmas informações sobre as mesmas vulnerabilidades. Ou seja não havia interoperabilidade entre as bases de dados das diversas ferramentas de segurança. Cada vendedor de ferramentas de segurança definia as métricas tornando-as diferentes para todas as ferramentas. A CVE resolveu estes problemas pois normaliza as métricas que são fornecidas pelas ferramentas. É conhecida como a entidade produtora de normas para os nomes das vulnerabilidades (Mitre, 1999).

Esta norma fornece pontos de referência para a troca de dados tornando possível a comunicação entre produtos e serviços da área da segurança da informação. Proporciona, inclusive, um guia para as organizações efetuarem uma avaliação sobre as suas ferramentas ou serviços (Mitre, 1999).

2.4.2 Common Vulnerability Scoring System

Common Vulnerability Scoring System (CVSS) é uma *framework open source* utilizada para a comunicação das características e o impacto que as vulnerabilidades,

na área das Tecnologias de Informação (TI), podem ter na organização. Inicialmente a sua conceção foi para uma utilização na priorização de desenvolvimento de *patch.* Contudo, após avaliação do potencial, foi sendo utilizado num espectro alargado. O objetivo é permitir uma valorização das vulnerabilidades do sistema informático ou de informação, proporcionando aos utilizadores uma clara e intuitiva representação dessa mesma vulnerabilidade. O CVSS, tipicamente, é utilizado por gestores de TI, fornecedores de soluções de segurança, fornecedores de aplicações, investigadores entre outros *players* da área. Para fornecer a valorização das vulnerabilidades, o CVSS baseia-se em três conjuntos de métricas: Base, Temporal e Ambiental. Para além de se obter um *score* compreendido entre 0 e 10, o CVSS fornece uma representação textual que reflete os valores utilizadores para atingir esse mesmo *score* (Mell et al., 2007). Os conjuntos de métricas para cada grupo são apresentados na Figura 8.

Figura 8 – Grupos de Métricas do CVSS (Baseado em: Mell et al. (2007))

O conjunto de métricas Base representa as características intrínsecas e fundamentais de uma vulnerabilidade sendo essas constantes ao longo do tempo e no mesmo ambiente de trabalho. O conjunto de métricas Temporais representa as características de uma vulnerabilidade que mudam ao longo do tempo, mas não se altera entre diferentes ambientes de trabalho. O conjunto de métricas Ambiental representa as características de uma vulnerabilidade que é única para qualquer ambiente de trabalho.

Os utilizadores, com base nos três conjuntos de métricas apresentados (Figura 8), podem ter acesso a informação contextual mais específica e fiável que pode refletir risco para o ambiente de trabalho da empresa (Mell et al., 2007). Esta situação permite aos gestores tomarem uma decisão, baseada em informação fiável, de modo a mitigar o risco a que estão expostos e que foi deliberado pela análise das vulnerabilidades.

2.4.3 Common Configuration Scoring System

Common Configuration Scoring System (CCSS), proposto pela NIST, é um conjunto de métricas, vocacionadas para a medição das vulnerabilidades das configurações de *softwares* de segurança (Mell et al., 2007). Este conjunto foi desenvolvido com base no CVSS descrito anteriormente. O CCSS auxilia as organizações na tomada de decisão quanto à forma como os problemas de configuração da segurança podem ser mitigados. Isto acontece através do fornecimento de dados que podem ser utilizados em avaliações quantitativas para definir a segurança geral de um sistema.

2.4.4 Compromise and Attack Level Monitor

O *Compromise and Attack Level Monitor* (CALM) é utilizado pelo OSSIM, e é considerado um algoritmo de avaliação que utiliza a acumulação de eventos recolhidos ao longo do tempo. O *input* para este algoritmo é o grande volume de eventos de segurança, e o *output* é um indicador singular que reflete o estado geral da segurança do sistema. A acumulação de eventos é verificada com a junção de

eventos provenientes de quaisquer equipamentos da rede incluindo qualquer máquina, grupo de máquinas, entre outros. Estes equipamentos têm que ser considerados interessantes do ponto de vista da monitorização dos ataques. A acumulação de eventos utilizada pelo CALM divide-se em dois grandes estados que representam o risco do sistema: Estado C ou nível de comprometimento, que reflete a probabilidade da máquina ou sistema estar comprometida; Estado A ou nível de ataque que reflete a probabilidade do sistema ser atacado. O CALM foi concebido para monitorização de ataques em tempo real avaliando eventos recentes (Karg et al., 2013).

2.4.5 Vulnerability Assessment Assurance Levels

O *Vulnerability Assessment Assurance Levels* (VAAL) foi criado por David Litchfield em 2006 e cinge-se a uma forma de comunicação devido à extensão da análise de segurança que tinha sido melhorada num produto. Esta forma de comunicação era também utilizada como guia para a realização de análises de segurança repetidas em várias camadas. Se o VAAL fosse totalmente integrado num *software* poderia ser benéfico para os consumidores que, normalmente, não têm as noções necessárias para avaliar a segurança de um produto. Pode constituir um componente de um *software* de segurança (Christey, 2007).

Christey (2007) especifica 9 dimensões que podem ser adotadas pelo VAAL para efetuar uma valorização de vulnerabilidades singulares. As dimensões propostas são: pressupostos para a maturidade do *Security Development Life Cycle* (SDLC), restrições de acesso, frequência, gravidade potencial, novidade, profundidade, complexidade da manipulação, ubiquidade e níveis de esforço.

Com estas dimensões é possível estabelecer métricas para a avaliação do *software* do ponto de vista da segurança. Pode também ser útil na análise de vulnerabilidade. As métricas que, num futuro, sejam definidas podem ser concebidas ao nível de vulnerabilidades individuais ou de grupos de vulnerabilidades (Christey, 2007).

2.5 Trabalho na área da Gestão de Eventos de Segurança da Informação

A área dos eventos de segurança da informação tem um forte potencial e tem sido alvo de diversos estudos científicos. A visualização de eventos, uma componente da GESI, tem sido a vertente mais focada pela comunidade científica. Outra vertente que tem sido focada, nos últimos anos, são os SIEM. Nesta secção pretende-se mencionar alguns trabalhos realizados nas vertentes acima mencionadas. São apresentados 4 trabalhos relacionados com a Visualização da Segurança da Informação e 3 trabalhos relacionados com a definição de requisitos para serem utilizados pelos SIEM.

2.5.1 Visualização da informação

O termo "Visualização", na área da segurança, é relativamente recente (Shiravi et al., 2012). Constitui-se uma ferramenta importante para a área. É caracterizada por ser um método de apresentação de um número elevado de registos, contendo informação, num relativo espaço curto (Kasemsri, 2006). A ideia principal é colocar um humano a visualizar os dados, retirar conclusões diretas ou indiretas através desses dados (Keim, 2002). Assim torna possível a identificação e análise de padrões ajudando na deteção de problemas ao nível da segurança da informação (Kasemsri, 2006). A visualização da segurança e, neste caso, dos eventos de segurança, constitui um importante processo de exploração de dados para detetar e resolver futuros incidentes (Barrera, 2009; Keim, 2002).

Pearlman e Rheingans (2007), efetuaram o seu trabalho focado na área da visualização dos eventos de segurança da informação. Mencionam algumas dificuldades sentidas na área da segurança, nomeadamente a deteção, a gravidade e o tipo de ataque que ocorre nas redes computacionais. Pearlman e Rheingans desenvolveram uma nova técnica de visualização com uma visão orientada a serviços. Esta técnica permite obter uma monitorização da atividade, na rede, ao longo do tempo. Com a utilização desta técnica, Pearlman e Rheingans afirmam que conseguiram detetar um *Denial-of-Service* (DoS). Estes investigadores contribuem para a comunidade científica através do fornecimento de uma aplicação que combina

algumas técnicas de visualização existentes. Essas permitem colmatar as dificuldades anteriormente mencionadas. Para validar a sua técnica de visualização efetuaram um *survey*. As respostas que obtiveram leva-os a crer que a sua técnica disponibiliza mais e melhor informação que as que existiam na altura.

Luse, Scheibe e Townsend apresentam uma nova estrutura que combina componente de visualização com componentes dos sistemas IDS. Os autores afirmam que a visualização da informação, tem sido explorada ao longo dos anos como um mecanismo de melhoria da análise dos IDS sobre o tráfego de rede. A estrutura pode ser utilizada no desenho e implementação de sistemas de visualização na deteção de intrusões. Os components de visualização são: *Overview, Zoom, Filter, Details On Demand, Relate, History* e *Extract, Primary Notification* e *Secundary Throughput*. Com uma análise sobre os sistemas de visualização e um *survey* elaborado sobre 23 projetos de investigação, os investigadores avaliaram a aplicação da estrutura criada (Luse, Scheibe, & Townsend, 2008).

Shiravi et al. (2012) expressam a ideia de que as técnicas de visualização comuns foram projetadas para casos de utilização e não são de suporte à segurança da informação. Exigem novas técnicas para a visualização com o propósito de conseguir-se uma análise minuciosa para a segurança da informação. Os autores efetuaram um *survey* detalhando 38 ferramentas de visualização da informação estando essas descritas na Tabela 5.

Tabela 5 – Sistemas de Visualização nos últimos 15 anos (Fonte: Shiravi et al. (2012))

Sistema de Visualização	Ano	Técnica (s) de Visualização	Fonte de dado
Monitorização de Servidores/*hosts*			
Erbacher *et al.*	2002	Glifo	*Logs* do Servidor
Tudumi	2002	Ligação em Nó, em 3D	*Logs* do Servidor
NvisionIP	2003	Dispersão	*NetFlows*
Portail	2005	Ligação em Nó	Interceção de pacotes
HoNe	2006	Ligação em Nó	Interceção de pacotes

Radial Traffic	2006	Painel Radial	Interceção de pacotes
Perlman *et al.*	2007	Ligação em Nó | Glifo	Interceção de pacotes
Mansmann *et al.*	2008	Ligação em Nó	Interceção de pacotes
Monitorização Interna/Externa			
VISUAL	2004	Dispersão | Matriz de IP	Interceção de pacotes
VizFlowConnect	2004	Coordenadas Paralelas	*NetFlows*
Erbacher *et al.*	2005	Painel Radial	Interceção de pacotes
TNV	2005	Matriz IP | Mapa de Cores	Interceção de pacotes
Atividade nos Portos			
Cube of Doom	2004	Dispersão em 3D	Interceção de pacotes
PortVis	2004	Dispersão	*NetFlows*
Abdullah *et al.*	2005	Histograma	Interceção de pacotes
NetBytes Viewer	2008	Dispersão em 3D	*NetFlows*
Existence Plots	2008	Dispersão	Interceção de pacotes
Padrões de Ataque			
Giardin	1999	Mapa de Cores	Interceção de pacotes
NIVA	2002	Ligação em Nó | Glifo	Alertas de Intrusão
Snort View	2004	Dispersão | Glifo	Alertas de Intrusão
IDGraphs	2005	Dispersão	*NetFlows*
IP Matrix	2005	Dispersão | Cores	Alertas de Intrusão
Visual Firewall	2005	Dispersão	Interceção de pacotes
IDS Rainstorm	2005	Dispersão	Alertas de Intrusão
Vizalert	2005	Painel Radial	Alertas de Intrusão
Rumint	2005	Coordenadas Paralelas	Interceção de pacotes
Ren et *al.*	2006	*Flying Term*	Interceção DNS
Xiao *et al*.	2006	Dispersão	Interceção de pacotes
Svision	2007	Dispersão em 3D	Interceção de pacotes
Mansmann *et al.*	2007	Mapa em Árvore	Interceção de pacotes
SpiralView	2007	Painel Radial	Alertas de Intrusão
NflowVis	2008	Mapa em Árvore	*NetFlows*
Avisa	2010	Painel Radial	Alertas de Intrusão
Comportamento do *Router*			

Teoh *et al.*	2002	Histograma | Ligação em Nó	Interceção BGP
BGPaly	2005	Ligação em Nó	Interceção BGP
Wong *et al.*	2005	Ligação em Nó	Interceção BGP
LinkRank	2006	Ligação em Nó	Interceção BGP
BGP Eye	2006	Mapa de Cores	Interceção BGP

Davey et al. (2012) referem a tecnologia *Visual Analytics* (Figura 9) como sendo a tecnologia que oferece novas formas de extração dos dados do *big data*. Essa tecnologia utiliza soluções inteligentes e interativas de internet e de segurança para esse efeito (Davey et al., 2012).

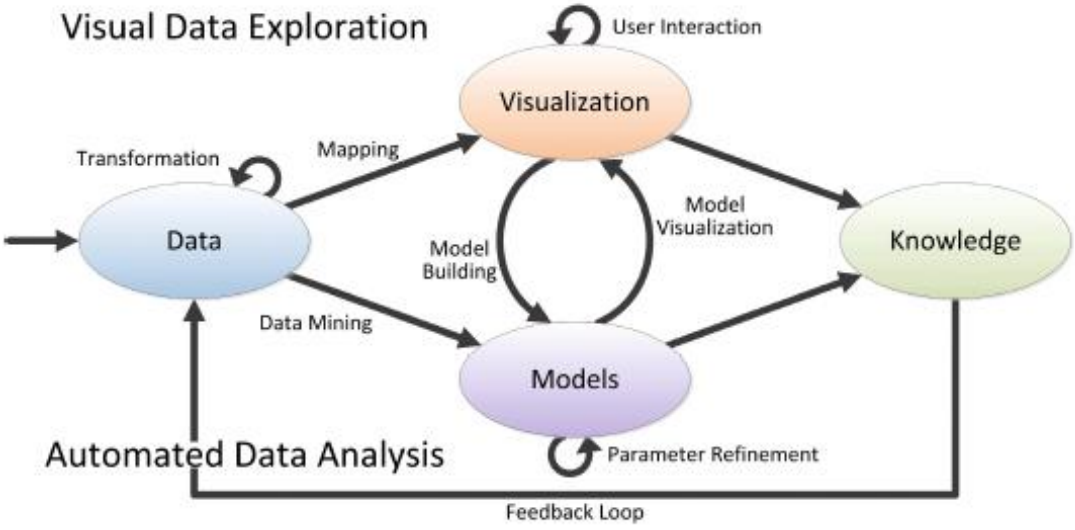


Figura 9 – O processo de *Visual Analytics* (Fonte: Davey et al. (2012))

A aplicação proposta por Fischer et al., em 2008, (citado por Davey et al. (2012)) o *NetFlows*, foi utilizada no trabalho com o objetivo de permitir rápidas perceções visuais sobre padrões de comunicação. Com a utilização da ferramenta, Davey et al., em 2012, demonstraram como a combinação automática e visual da análise de dados pode ajudar os especialistas de segurança a obterem, com maior rigor, os eventos de

segurança que ocorrem no elevado tráfego de rede das infraestruturas. Os autores mencionam ainda que a *Visual Analytics* tem uma importância extrema no desempenho das infraestruturas da rede da internet no futuro. O melhorar do apoio visual e computacional, do planeamento e dos testes à infraestrutura, da monitorização da rede e da segurança da rede, constituem-se como características do *Visual Analytics*. Este permitirá reagir de forma imediata a falhas ou ataques que são inerentes ao tráfego da rede.

2.5.2 Security Information Event Management (SIEM)

Atualmente, para a GESI, existem os SIEM como sendo os sistemas que fornecem serviços de segurança importantes para as organizações (Rieke et al., 2012). Esses sistemas recolhem e analisam eventos de segurança de diversas fontes (sensores, *firewalls*, routers, serves). Têm o objetivo de fornecer uma visão única sobre o estado de segurança do sistema de informação (Rieke et al., 2012). Os SIEM ajudam na tomada de decisão ou na análise antecipada do impacto sobre o que os eventos poderão causar na organização. Alguns investigadores debruçam-se sobre este tipo de sistemas, e não só, de modo a perceberem o seu funcionamento e a sua aplicabilidade, bem como para definirem requisitos para posterior utilização em SIEM de nova geração.

Pallotti e Mangiatordi (2011), não se debruçam sobre os SIEM. No entanto exploram os requisitos de segurança para a utilização dos *Smart Grid* (são sistemas que permitem a utilização, em conjunto, de tecnologias da informação e mecanismos de comunicação). Referem que estes sistemas estão a sofrer uma mudança substancial através da remoção de zonas débeis substituindo-as por zonas inteligentes. Esta situação leva a que hajam novas vulnerabilidades, através do sistema de comunicação e da distribuição elétrica. Os autores afirmam que o sistema passa a estar sujeito a alguns riscos como: um aumento do número de erros acidentais e potenciais ataques (quanto mais conexões existirem, mais vulnerável é o sistema); um aumento do número de entradas facilitando os ataques dos DoS; um aumento de falhas dos sistemas; e o possível aparecimento de novos problemas de segurança. Os autores afirmam que vários problemas para a segurança e privacidade aparecem com

os *Smart Grid*. Os clientes partilham mais informações sobre como pode ser utilizada a energia expondo-a a possíveis ataques. Assim, entendem que a Confidencialidade, a Integridade e a Disponibilidade (CIA) são os requisitos que um Smart Grid deve ter ao nível da segurança da informação. Sendo que, segundo os autores, a confidencialidade é um requisito do lado do cliente pois, a sua informação está registada em empresas que prestam serviços públicos e que passa a estar disponível no Smart Grid. O Smart Grid proporciona grandes benefícios para as empresas de serviços. No entanto, devido a alta conexão que possui, permite aos atacantes identificar e explorar as vulnerabilidades associadas à rede energética atacando diversos locais diferentes do Smart Grid.

Rieke et al. (2012) focam o seu trabalho na área dos SIEM. Estabelecem uma definição para estes sistemas e caracterizam quatro cenários: um evento desportivo, um serviço móvel de transferências monetárias, um serviço de gestão da infraestrutura numa grande empresa e um sistema de controlo de barragens. Nestes cenários, é possível aplicar um SIEM de modo a ajudar na análise de eventos de segurança. No primeiro cenário, mencionam inclusivamente os vinte mil tipos de eventos de segurança e os 11 milhões de eventos existentes num único dia de competição. Estabelecem requisitos de segurança da informação para serem incluídas na criação de novos SIEM, baseando-se na análise e aplicação dos quatro cenários mencionados e no SIEM correspondente. Os requisitos são: os eventos de segurança devem ser processados e respondidos em tempo real; a análise da informação de segurança do passado e do presente deve ser efetuada através da informação extraída dos eventos; a deteção de falsos positivos e negativos deve ser otimizada; as orientações sobre os requisitos mínimos para a correlação de eventos devem estar explícitas; as informações sobre o impacto da indisponibilidade de alguma informação sobre os eventos não estar disponível para a correlação e gestão de eventos; a recolha das informações sobre os eventos deve ser de fontes seguras e confiáveis; e melhorar o algoritmo de correlação de eventos para a utilização em ambientes complexos (automatização do processamento de correlação). Os autores criaram um modelo conceptual para conseguirem validar e demonstrar a sua abordagem. Esse modelo mostra a progressão de processos, aplicações e infraestruturas do negócio para elementos que podem ser utilizados no desenho e na

implementação de novos SIEM. Como conclusões, referem que a definição dos requisitos para a criação de novos SIEM não está completa. Contudo, afirmam que existe uma probabilidade elevada do seu trabalho poder ser direcionado para a definição de uma ampla variedade de requisitos para novos SIEM. Os mesmos autores referem o benefício de terem utilizado cenários múltiplos, pois os requisitos mencionados podem ser aplicados a uma grande variedade de contextos dentro da área da GESI.

Schütte et al. (2012) focam o seu trabalho na definição de um modelo para a GESI Os eventos da rede e a sua correlação não estão interligados a um modelo de segurança que seja consensual na comunidade. Os modelos atuais não conseguem incluir, como um todo, requisitos de conformidade, contramedidas e de avaliação da perda de informação. Segundo os autores, os SIEM atuais são focados para a deteção de intrusões, tipicamente funções associadas a um *Intrusion Detection System* (IDS). Assim, a contribuição efetuada pelos autores é a proposta de um modelo semântico para a GESI. Esse modelo é criado com base em 5 requisitos: a linguagem de processamento dos eventos deve ser abstrata; a correlação deve ser transversal entre os níveis de segurança e os incidentes; a inclusão do contexto da informação de segurança; o modelo deve reagir a incidentes de segurança; e a retroatividade da rastreabilidade de requisitos de segurança deve ser efetuada. Segundo os autores, a adoção deste modelo semântico permite a identificação dos incidentes, a definição de contramedidas, permite ligações a modelos de segurança externos e, também, efetua a correlação de eventos com diversas fontes.

2.6 Conclusão

Os eventos de segurança, tanto a nível de visualização como a nível dos SIEM, estão cada vez mais a chamar atenção dos investigadores. Pode-se verificar que, nesses níveis, existem soluções bastante razoáveis. A visualização dos eventos de segurança da informação, através dos *logs*, bem como a sua recolha e análise constituem um importante passo para a GESI. Nota-se a preocupação da definição de requisitos para a sua utilização na criação dos SIEM. No entanto, como transmitem Rieke et al. (2012), os requisitos e correspondente investigação pode ser direcionados para a

definição de uma ampla variedade de requisitos para serem incorporadas em novos SIEM. Sendo este trabalho de 2012 e tendo efetuado uma análise aos outros apresentados, conclui-se que nesta matéria, os mesmos são insuficientes.

Outra situação prende-se com o facto de nenhum dos autores, aqui apresentados, mencionam requisitos com base nas necessidades de um gestor de segurança da informação. A não existência de nenhum estudo que espelhe, claramente, os requisitos e dimensões que possam ser utilizadas numa nova solução e que vão de encontro ao que o gestor necessita de consultar, são também um problema na área da segurança da informação. Com este cenário, reforça-se o problema de não existe nenhum modelo que permite gerir o elevado número de eventos de segurança nos sistemas de informação. A resolução dos problemas retratados poderá ajudar os gestores a enfrentar os ataques com outra visão tendo a informação necessária para mitigar ou reduzir o seu impacto.

Considera-se que a dissertação irá trazer contributos à comunidade científica e empresarial.

3. Modelo para a Gestão de Eventos de Segurança da Informação

Após a análise da secção "Gestão de Eventos de Segurança da Informação", verifica-se a existência de diversos trabalhos na área dos eventos de segurança da informação. Os SIEM são as ferramentas fundamentais, atualmente, para a gestão dos eventos de segurança da informação. São esses que fornecem indicadores e métricas para ser possível efetuar uma medição sobre os eventos. Podendo um gestor de segurança da informação não ser técnico, torna-se difícil, perceber e interpretar a informação devolvida pelo SIEM.

A principal tarefa para a criação do modelo de GESI passa pela realização de um *survey* por parte de gestor de segurança da informação. Esse *survey* permite que surja um possível levantamento de requisitos para serem utilizados num modelo, ferramenta ou *framework* para a GESI.

3.1 *Survey* com foco na Gestão de Eventos de Segurança da Informação

Com a caracterização do problema, anteriormente apresentado, sente-se a necessidade da definição de requisitos sustentados nas necessidades de um gestor de segurança da informação. O *survey*[2] (Anexo A: *Survey***)** foi enviado a 97 profissionais da área da GSI, 34 dos quais responderam ao mesmo. Obteve-se uma taxa de respostas equivalente a 35 % do total de profissionais abordados. Os profissionais selecionados, para responderem ao *survey*, exercem profissão na área da segurança da informação. *Information Systems and Security Managers*, *Chief Information Security Officers*, *Security Managers*, *Information Security Managers e Director of Information Security* são alguns dos cargos profissionais dos inquiridos. O objetivo principal do *survey* é a identificação do que um gestor de segurança da informação necessita de consultar ao nível dos eventos de segurança da informação.

[2] No *survey* utiliza-se o conceito incidente por engano. No entanto, um incidente origina um ou mais eventos. Sendo assim, o *survey* assume como valido.

Os resultados obtidos foram analisados através da aplicação *Statistical Package for the Social Sciences* (SPSS), versão 14.0, fornecida pela IBM. Esta permite a transformação dos dados do *survey* em informação relevante para estudos científicos (IBM, 2013). A Tabela 6 apresenta os dados estatísticos do *survey* e nos quais serão baseados os requisitos.

Tabela 6 – Dados estatísticos gerais do estudo realizado

Resultados Gerais do *Survey*

Intenção da questão		Opção com mais seleção	Número de respostas	Percentagem de respostas
Nível de Segurança		Informação por níveis (baixo, médio, alto, muito alto, outros)	27	79.41%
Monitorização dos *Tickets*[3]		Sim	34	100%
Natureza dos Incidentes		Sim	31	91.18%
Histórico		Pelo menos 3 meses	14	41.18%
Scores		Sim	22	64.71%
Open Source		Não	30	88.24%
Vulnerabilidade	Acesso	Peso 6	11	32.35%

[3] Os *tickets* ajudam na resolução de incidências dentro das organizações. A abertura de um *ticket*, associado aos eventos de segurança da informação, pressupõe que exista uma resolução e posteriormente um fecho desse mesmo *ticket*.

dos sistemas de informação	Complexidade	Peso 4,5, 6	9	26.47%
	Autenticação	Peso 6	11	32.35%
	Impacto na Confidencialidade	Peso 6	22	64.71%
	Impacto na Integridade	Peso 6	16	47.06%
	Impacto na Disponibilidade	Peso 6	17	50.00%
Detalhe da Informação		Muito detalhada	23	67.65%

É possível visualizar, na Tabela 6, que a maioria das intenções das questões (10 em 16) têm uma resposta com, pelo menos, 50%. Esta situação reflete que o *survey* vai de encontro ao que os gestores de segurança da informação necessitam.

As intenções para as questões foram selecionadas com base em análises e pesquisas, sobre as funcionalidades de alguns SIEM (Nicolett e Kavanagh, 2013). Decide-se pela apresentação de uma única opção (a mais selecionada pelos inquiridos) pois entende-se que será essa a resposta que levará à definição dos requisitos apresentados nesta dissertação. Algumas das opções, denominadas de "Peso", revelam a quantificação da importância da questão no âmbito da gestão/análise de eventos de segurança da informação (sendo que o peso 1 é pouco relevante e o peso 6 constitui-se como muito relevante). As percentagens apresentadas revelam a quantificação daquela questão nas respostas totais dadas pelos inquiridos. Nota-se, inclusive, que o *survey* vai de encontro ao que os gestores necessitam pois algumas das questões irão refletir requisitos que já foram previamente definidos.

3.2 Requisitos e Dimensões

Através da análise do *survey* (Tabela 6), é possível efetuar-se o levantamento de requisitos. Os requisitos identificados são seis (Tabela 7). Este conjunto de requisitos são o que um gestor de segurança da informação considera relevante para a área da GESI. Para os requisitos são definidos objetivos e as respetivas dimensões que são utilizadas no Modelo de GESI. Os objetivos permitem identificar para que é necessária a informação da segurança. Sendo que, as dimensões permitem responder aos objetivo de modo a alcança-los.

Tabela 7 – Requisitos para um Modelo de GESI

Requisitos	Objetivo	Dimensões
Monitorizar os *tickets* associados aos eventos de segurança da Informação.	Identificar quantos *tickets* estão abertos, fechados ou em resolução.	Número de *tickets.*
A informação de segurança deverá ser disponibilizada por níveis e deverá ser possível visualizar desde o menor detalhe para o maior detalhe.	Conhecer o estado geral da segurança da informação.	Número de eventos críticos; Número Total de eventos.
Os eventos de segurança devem ser separados pela origem do evento.	Conter a perceção sobre a origem do evento (interno ou externo).	Número de eventos internos; Número de eventos Externos.
O tempo de histórico nunca pode ser inferior a 3 meses.	Identificar se o evento já ocorreu na organização ou não.	Frequência de eventos; Sequência dos eventos.
A consulta do histórico de	Identificar qual o	Frequência dos

eventos tem de, pelo menos, utilizar *scores*.	evento crítico que ocorreu mais vezes.	eventos no histórico
Das características da segurança, a confidencialidade terá que ser a mais importante para o sistema.	Ter conhecimento se existe quebra ou não na confidencialidade da informação critica.	Número de acessos ilegítimos à informação; Número Total de eventos.

Ao identificar os requisitos associa-se um objetivo e uma ou mais dimensões que respondem a esse objetivo (Tabela 7). O primeiro requisito advém da resposta dada pelos 34 gestores relativamente a existir ou não uma monitorização dos *tickets* associados aos eventos de segurança. A resposta foi positiva e unânime. O segundo requisito é retirado das questões que abordam a existência da informação de forma agregada e, se deveriam existir níveis de segurança para classificar a mesma. As respostas positivas têm percentagens elevadas (cerca de 79% e 68 % respetivamente). O terceiro requisito advém da necessidade que os gestores têm de saber quais são os eventos que têm origem dentro da organização ou fora da organização. A percentagem positiva de respostas é 91%. O quarto requisito permite ao gestor visualizar o que acontece à sua empresa nos últimos meses ou anos. Este requisito foi considerado o mais importante e por isso as respostas caem num histórico superior a 3 meses. O quinto requisito advém da necessidade que o gestor tem na visualização do histórico. Menciona-se no *survey* se os gestores querem ver o histórico com base na frequência dos eventos. As respostas positivas são da ordem dos 65 %. O sexto, e último requisito, foca as características da segurança da informação. Para o gestor a característica com mais relevância é a confidencialidade da informação e, por isso, obteve cerca de 65% das respostas dos gestores.

Ao nível dos objetivos, estes são definidos com base nos seis requisitos já apresentados. Para este estudo, cada requisito tem associado um objetivo. Os objetivos permitem ao gestor gerir a segurança numa perspetiva de gestão e não numa perspetiva técnica. O gestor não tem preocupações ao nível da deteção dos *tickets* mas, para ele, é fundamental saber os *tickets* que estão abertos, fechados ou

em resolução. Esta situação passa-se da mesma forma com o segundo objetivo. O gestor não necessita de saber como lhe conseguirão mostrar o estado geral da segurança da informação, contudo acha necessário ter esse conhecimento no exercício das suas funções. A quebra da confidencialidade é um vetor importante na análise. Ter algo que mostre se a confidencialidade da informação crítica foi afetada tem um contributo muito significativo para o ato de gestão, pois se a confidencialidade for garantida a dificuldade de existir um ataque com sucesso torna-se muito maior. Contudo não interessa saber como é criada, tecnicamente, a solução que fornece o resultado pretendido.

Ao nível das dimensões, cada objetivo contém uma ou mais dimensões que são necessárias para o alcançar. Foram definidas dez dimensões que estão conectadas com os seis objetivos. As dimensões revelam a informação que terá de ser retirada dos dados operacionais para ser tratada, cruzada e apresentada ao gestor de segurança da informação.

Os requisitos são baseados nas necessidades dos utilizadores/gestores. Através destes, temos a perceção que as necessidades são variadas. Desde a implementação de *tickets* passando por análises do histórico até ao conhecimento da quebra da confidencialidade da informação, o gestor obtém noções sobre os eventos que ocorrem na sua organização podendo, assim, optar pela melhor decisão para mitigar os impactos.

3.3 Modelo para a GESI

Após a estruturação e análise dos requisitos, objetivos e dimensões, nasce o Modelo para a GESI, ilustrado pela Figura 10. Este modelo é constituído por diversos componentes: Regulamentação para a segurança da Informação, Normas para a Segurança da Informação, Métodos de Avaliação e Classificação de Eventos de Segurança da Informação, Politicas de Segurança e o Processo de Análise do Evento.

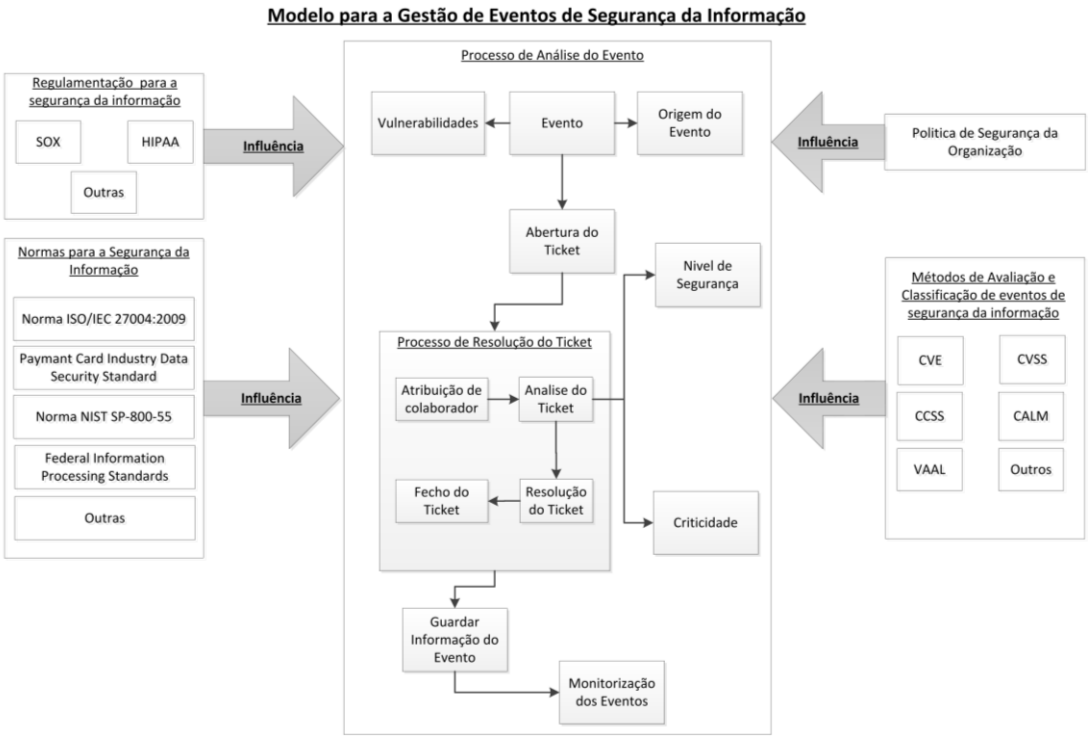


Figura 10 – Modelo para a GESI

O modelo apresentado pela Figura 10, visa essencialmente corrigir o problema identificado anteriormente. Contudo estima-se que tenha uma preponderância elevada na redução de falsos positivos devido a possuir, no início, uma análise e identificação de vulnerabilidades e origens do evento. Se um evento não explora nenhuma vulnerabilidade, numa organização qualquer, o gestor de segurança da informação pode compreender que não é prejudicial considerando-o como falso positivo. Um evento poderá, também, ser proveniente de determinadas zonas do globo onde já existem relatos de indícios de ataques à organização. Esta situação identifica o evento como critico. Se for o oposto, o gestor de segurança da informação pode sentir que é um falso positivo e, assim, elimina-o.

O modelo inclui quatro componentes que influenciam o processo de análise do evento (identificação da informação relacionada com um evento). A regulamentação apresentada e descritas na subsecção "Regulamentações aplicáveis na área da Segurança da Informação" tem influência na resolução e análise de um evento. Essa regulamentação têm várias funções dependendo da área e organização que as estão a implementar. No caso da HIPAA, este define padrões de segurança da informação e

obriga as organizações a monitorizarem os eventos associados à utilização da segurança. Na área financeira, o SOX obriga as organizações a tomar medidas de segurança da informação apropriadas e estabelecer diversos controlos em locais específicos do fluxo da informação, de modo a conseguirem fornecer a mesma.

As normas, apresentadas na subsecção "Normas para a Segurança da Informação", constituem-se como guiões que permitem a construção de métricas e indicadores de modo a existir eficiência na organização. As grandes instituições que têm operado nesta área, a ISO/IEC e a NIST, propõem variadíssimas normas para esta área. Para o modelo apresentado destacam-se duas normas: ISO/IEC 27004:2009 e a NIST SP-800-55. A norma ISO/IEC 27004:2009 permite às organizações avaliar diversos fatores (descritos na subsecção "Normas para a Segurança da Informação") que se tornam relevantes na GESI (ISO/IEC, 2009a). Por exemplo, verificar a métrica que indica se os requisitos de segurança definidos estão a ser cumpridos constitui-se muito importante para uma organização. Se os requisitos de segurança não são cumpridos existirá quebras de segurança. Permitirá, a um desconhecido, visualizar, extrair e apagar informação organizacional importante. A norma NIST SP-800-55 foi criada para assistir o desenvolvimento, seleção e implementação de métricas *core* de modo a essas serem utilizadas para a medição da segurança da informação (Chew et al., 2008).

Os métodos de avaliação e/ou classificação de eventos de segurança, mencionados na subsecção "Avaliação e Classificação de Eventos de Segurança da Informação", são ferramentas ou *frameworks* que tentam ajudar um colaborador de uma organização a avaliar e a classificar os eventos de segurança da informação que ocorrem no sistema de informação do seu empregador. Essas estão ligadas a vulnerabilidades existentes no sistema. O CALM, o CVSS, o CCSS e o VAAL efetuam, entre outros, a valorização das vulnerabilidades do sistema e a valorização das vulnerabilidades das configurações dos *softwares* de segurança. Todos os métodos de avaliação e/ou classificação estão ligados aos eventos de segurança da informação e influenciam a sua análise. São estes que permitem que seja possível o rastreio dos eventos críticos, através da deteção das vulnerabilidades, de modo a diminuir os falsos positivos (eventos detetados mas que não se constituem um problema para a organização).

A política de segurança da informação da organização, mencionada na subsecção "Conceito de Política de Segurança da informação", é a componente mais importante na área da segurança da informação (Whitman et al. em 2001, citado por J.Kenneth et al. (2009)). Ao nível destas políticas, menciona-se o que uma organização deve fazer no âmbito da segurança da informação. Estas devem refletir a ação a tomar quando existe uma deteção de eventos de segurança da informação. Se as politicas tiverem uma estrutura errada e a sua aplicabilidade é inexistente, é extremamente difícil a execução de tarefas e ações para prevenir e, até mesmo, mitigar possíveis danos causados por eventos e/ou ataques.

No modelo de GESI é possível visualizar que aos quatro componentes influenciadores mencionados poder-se-ão adicionar novas regulamentações, normas ou métodos de avaliação ou classificação, de modo a que o modelo seja moldável e expandido ao longo do espaço temporal.

O processo da análise do evento é a componente central e é constituída por quatro passos (Figura 11).

- Passo 1: Evento

  Este passo constitui-se pela deteção e análise do evento. Ao ser detetado o evento deve-se verificar se existe ou não uma vulnerabilidade associada a esse evento e se essa vulnerabilidade está ou não presente no sistema de informação. Se a resposta for negativa, constitui-se como um falso positivo. Seguidamente deve-se analisar a origem do evento. Esta verificação efetua-se através da existência ou não de uma relação entre o evento detetado e um que já tenho sido detetado no sistema e que esteja no histórico. Se a resposta for positiva significa que já existiu um evento no sistema com caracteristicas idênticas e a origem do evento idêntica. Pode-se consituir como um falso positivo desde que o anterior já tenho sido resolvido positivamente;
- Passo 2: Abertura do *Ticket*

  Após a análise do evento, se esse não se constituir como um falso positivo, então efetua-se a abertura de um *ticket* para, posteriormente, identificar uma solução de modo a corrigir as situações que esse evento poderá explorar e, até, originar um ataque;

- Passo 3: Processo de Resolução do Ticket

  Após a abertura do *ticket* é necessário resolver o mesmo e, por consequência, encontrar uma solução para o respetivo evento. Inicialmente é atribuído um colaborador que irá encarregar-se de efetuar uma análise do *ticket* (através da verificação do nível de segurança da organização e da criticidade do evento a analisar), delinear uma solução e fechar o *ticket* dando a indicação que o mesmo foi resolvido. A verificação do nível de segurança do sistema pressupõe que o colaborador tem uma ou várias ferramentas para o efeito que permitem verificar se a segurança geral da informação do sistema é baixa, média ou elevada (por exemplo a utilização de algumas técnicas de visualização propostas por (Shiravi et al., 2012)). A verificação da criticidade permite ao colaborador visualizar se o evento em causa é crítico para o sistema ou não. Esta criticidade é medida numa escala (a escala não está definida mas poderá ser valores numéricos, 0 a 1000, ou percentagens, 0% a 100%). Uma das opções para calcular a criticidade é a fórmula de cálculo da criticidade proposta por Rocha (2013). Esta fórmula inclui a perigosidade do evento, o tipo de ataque associado ao evento e a reputação do IP associado ao evento. Para fins de cálculo da perigosidade do evento, são utilizadas várias características dos mesmos: a idade da vulnerabilidade a explorar; o estado da vulnerabilidade; a severidade do ataque associado ao evento; a dificuldade de realização do ataque associado ao evento; o nível de perícia do atacante; o impacto do ataque associado ao evento quanto ao CIA; e o fator de risco associado à vulnerabilidade explorada pelo evento. Quanto maior o valor, que espelha a criticidade do evento, maior é a importância que o mesmo tem para o sistema. Após a análise efetuada, o colaborador esboça uma solução e resolve o *ticket* fechando o mesmo.
- Passo 4: Guardar Informação do Evento

  Este passo resume-se à alocação de toda a informação sobre o evento. Esta poderá ser guardada em bases de dados onde, *à posteriori*, poderá ser consultada.
- Passo 5: Monitorização dos Eventos

  Este será o último passo. Permite a existência de uma monitorização constante sobre os eventos que já estão alocadas em histórico. Isto é, à

medida que surgem os eventos, ir-se-á efetuar uma comparação com os eventos que já ocorreram na organização agilizando as respostas aos *tickets* dos eventos captados em cada instante.

Após a aplicação do modelo apresentado, existe uma fase onde são aplicadas as soluções resultantes deste mesmo modelo. Note-se que o modelo apresentado deverá constituir a sua aplicabilidade por evento e não por espaço temporal ou grupos de eventos. Com a aplicabilidade individual é permitida a resolução de cada evento crítico que seja despoletado pelo sistema. Permite rastrear e identificar os possíveis ataques através da redução de falsos positivos.

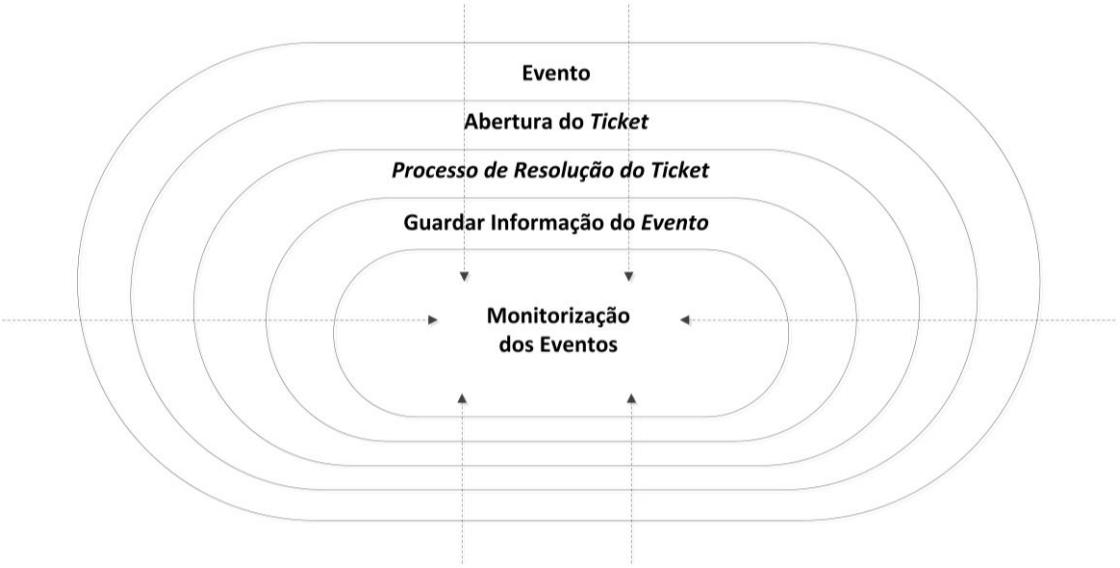


Figura 11 – O processo da análise de um evento

3.4 Conclusão

Após a apresentação do Modelo de GESI, verifica-se que as políticas de segurança, as normas, as regulamentações, as avaliações e as classificações de eventos de segurança da informação têm influência sobre a análise de cada um dos eventos detetados pelo sistema. O evento, com todas as suas características, é analisado como todas as restrições que os componentes circundantes impõem. Estas imposições são benéficas pois são internacionalmente reconhecidas e aplicadas em diferentes organizações com resultados de sucesso. Contudo, podem levar a alguns eventos

(que são críticos) sejam descartados pela análise efetuada devido ao seu estado não ser considerado crítico por determinada organização.

Outra situação prende-se com o facto de já existirem alguns requisitos (cerca de 15) definidos e mencionados. O modelo apresentado congrega 9 dos requisitos apresentados com os 6 requisitos definidos no âmbito desta dissertação. Os requisitos: as informações sobre o impacto da indisponibilidade de alguma informação sobre os eventos não estar disponível para a correlação e gestão de eventos; melhorar o algoritmo de correlação de eventos para a utilização em ambientes complexos (automatização do processamento de correlação); a linguagem de processamento dos eventos deve ser abstrata; a correlação deve ser transversal entre os níveis de segurança e os incidentes; e a retroatividade da rastreabilidade de requisitos de segurança deve ser efetuada, são requisitos importantes para a GESI. No entanto entende-se que estes serão utilizados na criação de uma ferramenta que venha a utilizar este modelo.

4. Discussão e Conclusão

Com a realização da investigação, ao abrigo da presente dissertação, verifica-se a necessidade da criação de um modelo para a GESI baseado em requisitos que sejam "definidos" por profissionais da área, os gestores de segurança da informação. O levantamento de requisitos do modelo elaborado tem como objetivo a análise de questões relacionados com os eventos de segurança da informação.

No âmbito dos eventos de segurança da informação, verifica-se a existência de trabalhos científicos, mais concretamente, ao nível da visualização e SIEM. O facto de existirem já alguns requisitos definidos, torna evidente a necessidade do aparecimento de novas ferramentas na área da GESI, aliás como menciona Rieke et al. (2012). Contudo, verifica-se que esses requisitos são definidos com base em cenários propostos pelos investigadores, ou com base nos conceitos fundamentais das propriedades da segurança da informação, o CIA. No entanto, em nenhum dos casos se verifica o contributo de pessoas que exerçam profissão na área, ou seja, os gestores de segurança da informação. Dai, apesar de alguns os requisitos definidos pelo trabalho decorrente desta dissertação (por exemplo o caso do CIA), nota-se que muitos dos mesmos não foram ainda contemplados.

Para o modelo criado, infelizmente, não foi possível validá-lo com dados reais de segurança da informação devido à escassez de tempo. No entanto assume-se que este semanticamente e teoricamente é válido devido à inclusão de normas, regulamentações e políticas de segurança da informação, à semelhança dos SIEM que são as ferramentas com que os gestores de segurança da informação utilizam atualmente ao nível da GESI. Além disso, a fonte do modelo também são os profissionais experientes da área através da utilização, por base, do *survey* elaborado.

5. Investigação Futura

O trabalho decorrente desta dissertação permite a investigadores e organizações utilizarem o modelo de modo a que sejam definidos mais requisitos e/ou que aumentem os componentes constituintes do modelo de GESI apresentado. Futuramente, o modelo deverá ser validado com dados reais obtidos num ambiente devidamente controlado. Pode-se, inclusive, aplicar o modelo em organizações de modo a efetuar alguns testes e a validar a sua usabilidade. Apesar de já se ter definido as normas e regulamentações, pode-se adicionar novas normas e regulamentações de diversos países que incidam sobre os eventos de segurança da informação (por exemplo a ISO/IEC 27000:2013). Isto permite a abrangência mundial por parte do modelo. Deve-se inclusive adicionar novos métodos de avaliação e/ou classificação de eventos de segurança da informação (à medida que surgem na comunidade empresarial e científica) de modo a conseguir-se extrair o máximo de informação possível sobre a ocorrência de um determinado evento. Por fim, utilizar este modelo com outros modelos de gestão que reflitam a gestão de ataques/incidentes de segurança da informação.

6. Referências Bibliográficas

Andrade, D., & Oliveira, M. (2012). Hackers acedem a dados pessoais de árbitros há, pelo menos, nove meses. *Jornal Público*. Retrieved from http://www.publico.pt/noticia/hacker-acede-a-dados-pessoais-de-arbitros-ha-pelo-menos-nove-meses-1538899

Barrera, D. (2009). *TOWARDS CLASSIFYING AND SELECTING APPROPRIATE SECURITY VISUALIZATION TECHNIQUES*. CARLETON UNIVERSITY.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). NIST Special Publication 800-55 Revision 1 - Performance Measurement Guide for Information Security. Gaithersburg, MD - EUA: National Institute of Standards and Technology.

Christey, S. (2007). Unforgivable Vulnerabilities. Bedford, EUA: MITRE Corporation.

Cloud Access. (2011). SIEM & Events per Second. Retrieved September 19, 2013, from http://www.cloudaccess.com/featured_articles/siem-events-per-second/

Davey, J., Mansmann, F., Kohlhammer, J., & Keim, D. (2012). Visual Analytics : Towards Intelligent Interactive Internet and Security Solutions. *The Future Internet Future Internet Assembly 2012: From Promises to Reality* (Vol. 7281, pp. 93–104). doi:10.1007/978-3-642-30241-1_9

Dekker, M., Karsberg, C., & Lakka, M. (2012). Annual Incident Reports 2012. Crete, Greece: European Union Agency for Network and Information Security (ENISA).

Eloff, J. A. N. (2003). Information Security Management – A New Paradigm. In J. Eloff, A. Engelbrecht, P. Kotzé, & M. Eloff (Eds.), *SAICSIT '03 Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* (pp. 130–136). Republic of South Africa.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10–16. doi:10.1016/S1361-3723(05)70275-X

Ericsson, G. (2004). Managing Information Security in an Electric Utility. *Electra Magazine - Cigré*, *216*.

Gilaninia, S., Mousavian, S. J., Taheri, O., Nikzad, H., Mousavi, H., & Seighalani, F. Z. (2012). Information Security Management on performance of Information Systems Management. *Journal of Basic and Applied Scientific Research*, *2*(3), 2582–2588.

Haymarket Media, I. (2013). SIEM. *SCMagazine 2013*. Retrieved from http://www.prismmicrosys.com/documents/SIEM_R2_ebook.pdf

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *Mis Quarterly*, 75–105.

Hong Kong Government. (2008). *AN OVERVIEW OF INFORMATION SECURITY STANDARDS*. Hong Kong, Japan.

Howard, J. D., & Longstaff, T. A. (1998). *A Common Language for Computer Security Incidents*. New Mexico - USA.

IBM. (2013). SPSS software Predictive analytics software and solutions. *IBM*. Retrieved from http://www-01.ibm.com/software/analytics/spss/

ISO/IEC. (2009a). ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement. Geneva, Switzerland: International Commission Organization for Standardization/International Electrotechnical.

ISO/IEC. (2009b). ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: International Commission Organization for Standardization/International Electrotechnical.

J.Kenneth, K., Franklin, M. R. J., Thomas, E. M., & Byrd Terry Anthony. (2009). Information security policy: An organizational-level process model. *Elsevier*, *28*(7), 493–508.

Karg, D., Muñoz, J. D., Gil, D., Ospitia, F., González, S., & Julio Casal. (2013). OSSIM Open Source Security Information Management - General System Description.

Kasemsri, R. R. (2006). *A Survey, Taxonomy, and Analysis of Network Security Visualization Techniques*. Georgia State University.

Keim, D. A. (2002). Information visualization and visual data mining. *IEEE Transactions on Visualization and Computer Graphics*, *8*(1), 1–8. doi:10.1109/2945.981847

Laxmidas, D. (2012). Botnet rouba 36 milhões de euros na Europa. *EXAME Informática*. Retrieved September 15, 2013, from http://exameinformatica.sapo.pt/noticias/internet/2012/12/07/botnet-rouba-36-milhoes-de-euros-na-europa

Luse, A., Scheibe, K. P., & Townsend, A. M. (2008). A Component-Based Framework for Visualization of Intrusion Detection Events. *Information Security Journal: A Global Perspective*, *17*(2), 95–107. doi:10.1080/19393550802039791

Martins, A. ., & Santos, C. A. S. (2005). Uma Metodologia para Implantação de Um Sistema de Gestão de Segurança da Informação. *Journal of Information Systems and Technology Management*, *2*(2), 121–136.

Mell, P., Scarfone, K., & Romanosky, S. (2007). CVSS - A Complete Guide to the Common Vulnerability Scoring System. North Carolina, USA.

Mitre. (1999). Common Vulnerabilities and Exposures - CVE The Standard for Information Security Vulnerability Names. Bedford, EUA: The MITRE Corporation.

Nicolett, M., & Kavanagh, K. M. (2013). Magic Quadrant for Security Information and Event Management, (May).

Pallotti, E., & Mangiatordi, F. (2011). Smart grid cyber security requirements. *2011 10th International Conference on Environment and Electrical Engineering* (pp. 1–4). IEEE. doi:10.1109/EEEIC.2011.5874822

Pearlman, J., & Rheingans, P. (2007). Visualizing Network Security Events Using Compound Glyphs from a Service-Oriented Perspective. In J. R. Goodall, G. Conti, & K.-L. Ma (Eds.), *VizSEC 2007* (p. pp 131–146). Sacramento, CA, USA: Springer Berlin Heidelberg.

Pedro, C. (2012). Como se roubaram 36 milhões de euros de contas bancárias este ano em 4 países. *Jornal de Negócios*. Retrieved September 15, 2013, from http://www.jornaldenegocios.pt/empresas/banca___financas/detalhe/como_se_roubaram_36_milhoes_de_euros_de_contas_bancarias_este_ano_em_4_paises.html

Rieke, R., Coppolino, L., Hutchison, A., Prieto, E., & Gaber, C. (2012). Security and Reliability Requirements for Advanced Security Event Management. *6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS* (pp. 171–180). St. Petersburg, Russia. doi:10.1007/978-3-642-33704-8_15

Rocha, M. (2013). *Modelo para definição de criticidade em eventos de segurança*. Minho University.

Schütte, J., Rieke, R., & Winkelvos, T. (2012). Model-Based Security Event Management. In I. Kotenko & V. Skormin (Eds.), *Computer Network Security* (p. pp 181–190). St. Petersburg, Russia: Springer Berlin Heidelberg.

Séneca, H. (2012). Portais do Governo sofreram mais de 800 mil ataques em agosto. *EXAME Informática*. Retrieved September 15, 2013, from http://exameinformatica.sapo.pt/noticias/internet/2012/09/19/portais-do-governo-sofreram-mais-de-800-mil-ataques-em-agosto

Shiravi, H., Shiravi, A., & Ghorbani, A. a. (2012). A survey of visualization systems for network security. *IEEE transactions on visualization and computer graphics*, *18*(8), 1313–29. doi:10.1109/TVCG.2011.144

Tangil, G. S., Palomar, E., & Julie, U. (2013). TOWARDS AN INTELLIGENT SECURITY EVENT INFORMATION MANAGEMENT SYSTEM. Madrid: Carlos III University of Madrid.

Techopedia. (2013). Events Per Second (EPS). Retrieved September 18, 2013, from http://www.techopedia.com/definition/23919/events-per-second-eps

Vaishnavi, V., & Kuechler, B. (2004). Design Science Research in Information Systems. *Association For Information Systems*. Retrieved from http://www.desrist.org/design-research-in-information-systems/

Viera, D. A. C., Castillo, A. L. M., & Chicaiza, J. V. T. (2012). *IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN Y ADMINISTRACIÓN DE SEGURIDAD PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA UNIVERSIDAD CENTRAL DEL ECUADOR (DTIC)*. UNIVERSIDAD CENTRAL DEL ECUADOR.

7. Anexo A: *Survey*

Title: Information Security Management

Initial Text

The survey comes as part of a dissertation in the area of information security at Minho University. Its main purpose will be to survey the requirements that the Manager of Information Security have in the management of information security evetns. Currently, we believe that the most widely used models are targeted for systems administration (most technical) and not for security management. With power requirements will prepare a management model information security incident, more appropriate, to current threats organizations. The questionnaire consists of rapid response questions and the time spent to resolve, on average, does not exceed 4 to 5 minutes. This research is being conducted under the Algoritmi Center, Minho University, and under the scientific guidance of Prof. Henrique Santos (hsantos@dsi.uminho.pt).

Thank you for the time you spent with this survey. Best Regards

Sidónio Seixas

Student of Master of Engineering and Management of Information System

Minho University

Questions:

Question 1: Organization size

Options: [<500]; [500-5000]; [5001-9500]; [9501-14000]; [>14000]

Question 2: Age of Manager Information Security

Options: [<30]; [31-40]; [41-50]; [51-60]; [61-65]; [>65]

Question 3: Location of organization's headquarters

Options: [Europe]; [Asia]; [North America]; [Central America]; [South America]; [Africa]; [Oceania]

Question 4: In the analysis of incidents you prefer?

Options: [Information on levels (low, medium, high, very high, others)]; [Information for actual value (100, 200, 500, 1000, etc.)]

Question 5: From the point of view of incidents management, tickets should be monitored?

Options: [Yes]; [No]

Question 6: In your opinion, should separate incidents with internal origin of the incidents that come from external sources?

Options: [Yes]; [No]

Question 7: The division of the system, in more specific areas, should be guided by:

Options: [Any]; [Machines (computers, servers, routers, etc.)]; [Geographic areas (buildings, departments, branches, etc.)]; [Critical Areas of the System (IDS, Firewall, critical machines, etc.)]

Question 8: Until time lag is necessary to maintain the history?

Options: [1 month]; [3 month]; [6 month]; [1 year]; [More than 1 year]

Question 9: In reviewing the history, feel the need to perform queries based on scores?

Options: [Yes]; [No]

Question 10: The software you use to manage security is Open Source?

Options: [Yes]; [No]

Question 11: The following metrics can be used to classify the vulnerabilities used by cyber-attacks. Rate them when the weight they have on your organization.

Weights 1 to 6: 1 is the lowest weight and the highest weight 6. Access Vector (AV) - the source location of the incident; Access Complexity (AC) - the attack complexity associated; Authentication (Au) - frequency of occurrence of the events associated with the incident; Confidentiality Impact (C) - impact on confidentiality, Integrity Impact (I) - impact on integrity; availability impact (A) - impact on availability.

Options: [AV]; [AC]; [Au]; [C]; [I]; [A];

Question 12: In continuous monitoring of incidents you prefer to have the information:

Options: [Very detailed]; [Little detailed]

Final Text

Your response was recorded. Thank you!

Best Regards

Sidónio Seixas